Elementary Number Theory
Lecture Notes

Lior Silberman

These are rough notes for the fall 2009 course. Solutions to problem sets were posted on an internal website. They are based on the textbook by Niven-Zuckerman-Montgomery.

Contents

CHAPTER 1

Introduction (9/9)

Lior Silberman, lior@Math.UBC.CA, http://www.math.ubc.ca/~lior
Office: Math Building 229B
Phone: 604-827-3031

1.1. Introduction

Two main themes of number theory: study of individual numbers, solution of equations in the integers.

1.1.1. Classical statements.

DEFINITION 1. Given an integer n set $\sigma(n) = \sum_{d|n} d$. Call n *deficient, perfect or abundant* if $\sigma(n)$ is less than, equal to, or larger than, $2n$, respectively.

EXAMPLE 2. $6, 28, 496, 8128$ are perfect number.

CONJECTURE 3. *There are infinitely many perfect numbers.*

PROBLEM 4. Are there any odd perfect numbers?

1.1.2. Results of numbers theory – Diophantine approximation.

THEOREM 5. *(Liouville 1847) α algebraic of degree $d \geq 2$ then there exists $c = c(\alpha) > 0$ such that for all $p, q \in \mathbb{Z}$ with $q \neq 0$, $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d}$.*

(Roth 1955) For all irrational algebraic α and $\varepsilon > 0$ there exists $c = c(\alpha, \varepsilon) > 0$ such that for all p, q $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{2+\varepsilon}}$

CONJECTURE 6. *(Oppenheim) Let $Q(\underline{x})$ be an indefinite quadratic form in $d \geq 3$ variables with real coefficients which is not a multiple of a form with rational coefficients. Then $Q(\mathbb{Z}^d)$ is dense.*

Circle method: $d \geq 21$ (Birch-Davenport-Ridout), $d \geq 5$ (Davenport-Heilbronn). Ergodic theory: Margulis.

CONJECTURE 7. *(Littlewood) Let α, β be irrational. Then* $\liminf_{n\to\infty} n \|n\alpha\| \|n\beta\| = 0$.

Easy to check this holds for (Lebesgue-)almost all α, β.

1.1.3. Results of numbers theory – prime numbers.

THEOREM 8. *(Euler) There are infinitely many primes.*
(Dirichlet) For $(a,q)=1$ there are infinitely many primes p so that $p \equiv a\,(q)$.

PROOF. (Euler) For $\Re(s)>1$ consider the infinite product $\zeta(s)=\prod_p (1-p^{-s})^{-1}$. It converges absolutely uniformly in every half-plane $\Re(s)\geq 1+\varepsilon$ since $\sum_p p^{-\Re(s)} \leq \sum_n n^{-1-\varepsilon} < \infty$. Direct calculation shows $\zeta(s)=\sum_{n=1}^{\infty} n^{-s}$. It follows that $\lim_{s\to 1}\zeta(s)=\infty$ (at least on the real axis). But if there were finitely many primes then $\zeta(s)$ would be continuous at $s=1$. □

THEOREM 9. *(Riemann) Under reasonable assumptions on the zeroes of $\zeta(s)$, $\#\{p \mid p\leq x\} = \frac{x}{\log x}+\tilde{O}(\sqrt{x})$.*
(de la Valee-Pussin; Hadamard) Unconditionally, $\#\{p \mid p\leq x\} \sim \frac{x}{\log x}$.
(Chebotarev) $\sum_{p\leq x,\, p\equiv a(q)} \log p \sim \frac{1}{\phi(q)}\frac{x}{\log x}$.

THEOREM 10. *(Fermat) A prime p is a sum of two squares iff $p \equiv 3\,(4)$ (actually a statement about primes in $\mathbb{Z}[i]$).*

1.1.4. Results of number theory – Diophantine equations. Linear equations:

CONJECTURE 11. *(Goldbach 1742) For all even $n\geq 4$ the equation $p_1+p_2=n$ has a solution with p_i prime.*

THEOREM 12. *(Vinogradov 1937) All sufficiently large odd n are sums of three primes.*

Quadratic equations:

THEOREM 13. *(Fermat) An integer n is a sum of two squares iff ...*
(Legendre 1798 + Gauss) An integer is a sum of three squares iff ...
(Lagrange 1770) Every non-negative integer is the sum of four squares.
(Jacobi) $r_4(n)=\sum_{d|n,\,4\not|\,d} d$.
(Bhargava-Hanke) A positive-definite integral quadratic form represents every integer iff it represents every integer up to 290.

More complicated equations

THEOREM 14. *(Greeks) The equation $x^2+y^2=z^2$ has infinitely many primitive solutions.*
(Fermat) The equation $x^4+y^2=z^4$ has no non-trivial solutions.
(Frey-Serre-Ribet, "FLT") For $n\geq 3$ there are no rational points on the curve $x^n+y^n=1$.

General equations

CONJECTURE 15. *(Waring 1770) For all $k\geq 1$ there exists $g(k)$ such that every $n\geq 0$ is the sum of at most $g(k)$ kth powers.*

Basically resolved by the circle method.

1.1.5. Discussion. Classical notions versus modern formulation. Congruences or equations in $\mathbb{Z}/m\mathbb{Z}$?

1.2. Technical stuff

None really except for the notion of an abelian group.

1.2.1. Course plan.

- $\mathbb{Z}/m\mathbb{Z}$.
- Prime numbers, arithmetical functions.
- Continued fractions and Diophantine approximation.
- Other topics

We will pay attention to the algorithmic complexity of some results.

1.3. Initial definitions (14/9) [1, §1.2]

1.3.1. The integers. Start with theory of the integers. Traditionally people worked with the natural numbers.

DEFINITION 16. Say that *a divides b* (or that *b* is a *multiple* of *a*) and write $a|b$ if there exists c so that $b = ac$. Say that a is a *unit* if it divides 1.

For $m \in \mathbb{Z}$ write (m) or $m\mathbb{Z}$ for the set of multiples of m.

LEMMA 17. *(divisibility)*

- $a|b$ *implies* $a|bc$ *for all* c.
- $a|b$ *and* $a|c$ *implies* $a|b+c$.
- *For* $c \neq 0$, *we have* $a|b$ *iff* $ca|cb$.
- $a|b$ *implies* $|a| \leq |b|$. *In particular,* $\{\pm 1\}$ *are the only units of* $\mathbb{Z}$.

The first two properties can be summarized as:(m) *is closed under addition and under multiplication by arbitrary elements of* $\mathbb{Z}$. *Non-empty subsets with this property are called* ideals.

COROLLARY 18. *The relation* $a \equiv b\,(m)$ *defined by* $a - b \in (m)$ *is an equivalence relation. The relation is called* congruence modulu *m; the equivalence classes are called* congruence *(or* residue*) classes modulu m. We write* $[a]_m$ *or* $a + m\mathbb{Z}$ *for the congruence class of a modulu m, and* $\mathbb{Z}/m\mathbb{Z}$ *for the set of equivalence classes.*

REMARK 19. We say r is a *residue of* b modulu m if $r \equiv b\,(m)$. Classically one worked in terms of residues. However, it is much better to think in terms of residue classes, *identifying* congruent numbers. Exceptions will arise, especially for analytic number theory.

THEOREM 20. *(Division with remainder) Let* $a, b \in \mathbb{Z}$ *with* $a \neq 0$. *Then there exist unique* $q, r \in \mathbb{Z}$ *with* $0 \leq r < |a|$ *such that*

$$b = qa + r\,.$$

PROOF. Let r be the least non-negative member of $b + a\mathbb{Z}$ (note that $b + |ab| \geq 0$). Then $r < |a|$ (else $r - |a|$ would be a smaller non-negative member of the residue class). Then $b - r \in a\mathbb{Z}$. If $qa + r = q'a + r'$ then $r - r' \in (a)$, and if they are distinct it follows that $|r - r'| \geq |a|$. It follows that $r = r'$ and hence that $q = q'$. □

REMARK 21. Note that this gives an algorithmic prescription for finding q and r given a and b by repeatedly subtracting a (or $-a$) from b so that the resulting number moves toward the range

COROLLARY 22. *(*$\mathbb{Z}$ *is a PID) Let* $I \subset \mathbb{Z}$ *be an additive subgroup (in particular, an ideal). Then* $I = (a)$ *for some* $a \in \mathbb{Z}_{\geq 0}$.

PROOF. If $I = (0)$ there is nothing to prove. Otherwise I has positive members. Letting a be the least such member, we have $(a) \subset I$ by induction. Finally, write any $b \in I$ in the form $b = qa + r$ as above. Then $r = b - qa \in I$ and $0 \leq r < a$. By the choice of a we conclude that $r = 0$, that is $b \in (a)$. □

DEFINITION 23. Let $S \subset \mathbb{Z}$ be finite and non-empty. Write $\gcd(S)$ for the *greatest common divisor* $\max\{a \geq 1 \mid \forall b \in S : a|b\}$ (except that if $S = \{0\}$ set $\gcd(S) = 0$), $\operatorname{lcm}(S)$ for *least common multiple* $\min\{a > 0 \mid \forall b \in S : b|a\}$ (except that if $0 \in S$ or S is unbounded set $\operatorname{lcm}(S) = 0$).

We have defined the gcd *multiplicatively*.

DEFINITION 24. Write(S) for the *ideal generated by S*, that is $\cap_{S \subset I \lhd \mathbb{Z}} I$.

PROPOSITION 25. $(S) = \left\{\sum_{s \in S} f(s) \cdot s \mid f \colon S \to \mathbb{Z}, \#\left(S \setminus f^{-1}(0)\right) < \infty\right\}$. *Also,* $(S) = (\gcd(S))$. *Finally,* $(\operatorname{lcm}(S)) = \cap_{s \in S}(s)$.

PROOF. The first assertion is clear. For the second, let $a \in \mathbb{Z}_{\geq 0}$ be such that $(S) = (a)$. Then every $s \in S$ is a multiple of a, so that $a \leq \gcd(S)$. Conversely, by the first assertion every common divisor of S divides every element of (S) and hencegcd$(S) \leq a$. Finally, the ideal $\cap_{s \in S}(s)$ is the set of common multiples and the proof of the Corollary shows that its generator is its least positive member (or zero if the ideal is trivial). □

COROLLARY 26. *Every common divisor of S divides* $\gcd(S)$*; every common multiple of S is divisible by* $\operatorname{lcm}(S)$.

PROOF. Every common divisor of S divides every integer combination of elements of S, hence every member of (S). The second assertion follows from □

NOTATION 27. We sometimes write (S) for the gcd of the set S rather than for the ideal generated by S. Using (S) for the gcd and $[S]$ for the lcm is, in fact, the traditional notation.

DEFINITION 28. Call $S \subset \mathbb{Z}$ *relatively prime* if $(S) = (1)$.

LEMMA 29. *(Euclid) Let $a, b \in \mathbb{Z}$ and write $a = qb + r$ for some $q, r \in \mathbb{Z}$. Then $(a, b) = (b, r)$, and in particular $(a, b) = (a - b, b)$.*

ALGORITHM 30. *(Euclid) Two versions: one using subtraction, the other using division with remainder.*

1.3.2. $\mathbb{Z}/m\mathbb{Z}$**.**

LEMMA 31. *Setting $0_m = [0]_m$, $1_m = [1]_m$, $[a]_m + [b]_m \stackrel{def}{=} [a + b]_m$, $[a]_m \cdot [b]_m \stackrel{def}{=} [ab]_m$ makes $(\mathbb{Z}/m\mathbb{Z}, 0_m, 1_m, +, \cdot)$ into a ring. The map $a \mapsto [a]_m$ is a ring homomorphism.*

Math 437/537: Problem set 1 (due 16/9/09)

Euclid's Algorithm

1. Find the gcd and lcm of 1728 and 496. Show a complete calculation by hand.

The Fibonacci sequence

2. Define numbers f_n by $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$ for all $n \geq 1$. Show that $f_n \leq 2^n$ for all n. Conclude that the formal power series $F(x) = \sum_{n=0}^{\infty} f_n x^n$ has a positive radius of convergence.

3. Show that $F(x) = \frac{x}{1-x-x^2}$ (at least in the domain of convergence). Using the formula $\frac{1}{1-\alpha x} = \sum_{n=0}^{\infty} \alpha^n x^n$ find a closed-form expression for f_n.

4. Show that $\frac{\varphi^n}{\sqrt{5}} - 1 < f_n < \frac{\varphi^n}{\sqrt{5}} + 1$ where φ is the larger root of $t^2 - t - 1 = 0$.

5. Show that Euclid's algorithm for finding $\gcd(a,b)$ using divisions with remainder requires at most $\log_{\varphi}(\max\{a,b\})$ divisions.

Divisibility

Only use results about divisibility for this section; do not invoke the notion of a prime.

6. (More gcd identities)
   (a) Let $a, b \in \mathbb{Z}$ be relatively prime. Show that any divisor c of ab can be uniquely written in the form $c = a'b'$ with $a'|a$, $b'|b$.
   (b) Show that $\gcd(a,bc) = \gcd(a,b) \cdot \gcd(a,c)$ for any $a,b,c \in \mathbb{Z}$ with b,c relatively prime.
   (c) Show that if $\gcd(a,b) = \gcd(a,c) = 1$ then $\gcd(a,bc) = 1$.

7. Let $x, a, b \in \mathbb{Z}_{\geq 1}$.
   (a) Show that $\gcd\left(x^a - 1, x^b - 1\right) = x^{\gcd(a,b)} - 1$.
   (b) Find $\gcd\left(x^a + 1, x^b + 1\right)$.

Algebra

8. Let A be a finite abelian group. For $x \in A$ and $d \in \mathbb{Z}$ write $d \cdot x$ for the sum of d copies of x (or $-d$ copies of $(-x)$ if $d < 0$).
   (a) For an integer d show that $A[d] = \{x \in A \mid d \cdot x = 0\}$ is a subgroup.
   (b) Show that $\sum_{x \in A} x = \sum_{x \in A[2]} x$.

9. For a prime p show that $(p-1)! \equiv -1\,(p)$.

Using the Gaussian Integers

For a complex number $z = x + iy$ write $\bar{z}$ for its complex conjugate $x - iy$, and Nz for its *norm* $z\bar{z} = x^2 + y^2$. We will study the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

10. Show that $\mathbb{Z}[i]$ contains $0, 1 \in \mathbb{C}$and is closed under addition and multiplication, in other words that it is a subring of $\mathbb{C}$. Establish the *well-ordering principle of* $\mathbb{Z}[i]$: a non-empty subset $S \subset \mathbb{Z}[i]$ contains $a \in S$ so that $Na \leq Nb$ for all $b \in S$.

11. (Sums of two squares) Say that $A \in \mathbb{Z}$ is *the sum of two squares* if there exist $a, b \in \mathbb{Z}$ so that $a^2 + b^2 = A$, that is if $A \in \{Nz \mid z \in \mathbb{Z}[i]\}$.
    (a) Show that $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ for all $z_1, z_2 \in \mathbb{C}$. Conclude that the norm is multiplicative.
    (b) Let $A, B \in \mathbb{Z}$ be each a sum of two squares. Show that AB is a sum of two squares.

12. (Euclidean property)
    (a) Let $a, b \in \mathbb{C}$ with $Nb \geq Na > 0$ and $Nb > \frac{1}{2}Na$. Show that one of $\mathrm{Re}(ab), \mathrm{Im}(ab)$ has magnitude at least $\frac{1}{2}|a|^2$.
    (b) Under the same assumptions as in part (a), show that there exists $\varepsilon \in \{\pm 1, \pm i\}$ such that $N(b - \varepsilon a) < Nb$.
    (c) Show that for every $a, b \in \mathbb{Z}[i]$ with $a \neq 0$ there exist $q, r \in \mathbb{Z}[i]$ so that $b = qa + r$ and $Nr < Na$.

Unique factorization can fail!

13. Let $\mathbb{Z}[\sqrt{-5}] = \left\{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\right\}$.
    (a) Show that $N\left(a + \sqrt{-5}b\right) = a^2 + 5b^2$ satisfies $N(z_1 z_2) = Nz_1 \cdot Nz_2$ for all $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$. Conclude that if $z \in \mathbb{Z}[\sqrt{-5}]$ is a unit (divides 1) then $z \in \{\pm 1\}$.
    Hint: Show that if $z|1$ then $Nz|N1$.
    (b) Show that every $z \in \mathbb{Z}[\sqrt{-5}]$ can be written as a product of irreducibles.
    (c) Show that $2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ in $\mathbb{Z}[\sqrt{-5}]$.
    (d) Show that no $z \in \mathbb{Z}[\sqrt{-5}]$ has norm 2 or 3. Conclude that $2, 3, \left(1 + \sqrt{-5}\right), \left(1 - \sqrt{-5}\right)$ are all irreducible there. Verify that no two are associates.

1.4. Primes and unique factorization (16/9/09) [1, §1.3]

- Irreducibles and decomposition into irreducibles; examples of $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Q}[x]$.
- Euclid: Infinitely many irreducibles; this shows $\pi(x) \ll \log\log x$.
- Primes. Unique factorization. Invertibility modulu irreducibles implies that irreducibles are prime. Unique factorization in $\mathbb{Z}$, $\mathbb{Z}[i]$ but $2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

1.5. Prime number estimates (16-20/11/09)

Idea: dyadic decomposition.

EXAMPLE 32. To estimate $\sum_{n\le x}\frac{1}{n}$ note that

$$\frac{1}{2} - o(1) = \frac{y-1}{2y} \le \sum_{y\le n\le 2y}\frac{1}{n} \le \frac{y+1}{y} = 1 + o(1).$$

Thus

$$\sum_{n\le x}\frac{1}{n} = \sum_{j=0}^{\log_2 x}\sum_{2^{-j-x}x\le n\le 2^{-j}x}\frac{1}{n}$$

means

$$\frac{1}{2}\log_2 x - C \le \sum_{n\le x}\frac{1}{n} \le \log_2 x + C.$$

LEMMA 33. *(Central binomial coefficients). We have* $\frac{1}{2n+1}4^n \le \binom{2n}{n} \le 4^n$

(1) $0 \le \operatorname{ord}_p\left(\frac{2n}{n}\right) \le \log_p 2n$. *In particular,* $\binom{2n}{n}$ *is an integer*
(2) *If* $p > \sqrt{2n}$ *then* $\operatorname{ord}_p\left(\frac{2n}{n}\right) \le 1$.
(3) *If* $p > n$ *then* $\operatorname{ord}_p\left(\frac{2n}{n}\right) = 1$.
(4) *If* $\frac{2n}{3} < p \le n$ *then* $\operatorname{ord}_p\left(\frac{2n}{n}\right) = 0$ *unless* $n = p = 2$.

PROOF. We use $2^{2n} = (1+1)^n = \sum_{k=0}^{2n}\binom{2n}{k}$. Setting $k = n$ gives the upper bound. For the lower bound note that the average of a sequence is at most the largest member.

For the rest, we use $\operatorname{ord}_p(n!) = \sum_{j=1}^{\infty}\left\lfloor\frac{n}{p^j}\right\rfloor$. Thus $\operatorname{ord}_p\binom{2n}{n} = \sum_{j=1}^{\infty}\left(\left\lfloor\frac{2n}{p^j}\right\rfloor - 2\left\lfloor\frac{n}{p^j}\right\rfloor\right)$. This is non-negative since each term is. In fact, $0 \le \left\lfloor\frac{2n}{p^j}\right\rfloor - 2\left\lfloor\frac{n}{p^j}\right\rfloor \le 1$. Summands with $j > \log_p 2n$ don't contribute so $\operatorname{ord}_p\left(\frac{2n}{n}\right) \le \log_p 2n$, and if $p > \sqrt{2n}$ then summands with $j > 1$ don't contribute. If $p > n$ then p divides the numerator once and the denominator not at all. If $\frac{2n}{3} < p \le n$ then $1 \le \frac{n}{p} < \frac{3}{2}$ and $2 \le \frac{2n}{p} < 3$ so the summand with $j = 1$ gives zero. The summand with $j = 2$ can only contribute if $\frac{2n}{p^2} \ge 1$ but $\frac{2n}{p^2} = \frac{1}{p}\frac{2n}{p} < \frac{3}{p}$. This can be at least one only if $p = 2$ and then $n \ge 2 > \frac{2n}{3}$ means $2 \le n < 3$. □

DEFINITION 34. Set $\nu(x) = \sum_{p\le x}\log p$, $\psi(x) = \sum_{n\le x}\Lambda(n) = \sum_{j=1}^{\infty}\nu(x^{1/j})$.

THEOREM 35. $\delta x \le \nu(x) \le \Delta x$ *where* $\Delta \le 2.18$ *and* $\delta = \frac{2\log 2}{3} - \frac{1}{3} > \frac{1}{8}$.

PROOF. Given x set $n = \lfloor \frac{x}{2} \rfloor$. Then the Lemma shows $\nu(x) - \nu(\frac{1}{2}x) \leq \log \binom{2n}{n} + \log x \leq x\log 2 + \log x$. We thus have:

$$\begin{aligned} \nu(x) &\leq x\log 2 \sum_{j=0}^{\infty} \frac{1}{2^j} + \frac{\log^2 x}{\log 2} \\ &\leq 2\log 2x + \frac{\log^2 x}{\log 2} \\ &\leq \Delta x \end{aligned}$$

since $\frac{\log^2 x}{x\log 2} \leq 0.785$ for all $x \geq 1$. Next, we have:

$$\log \binom{2n}{n} \leq \nu(x) - \nu(\frac{1}{2}x) + \nu(\frac{1}{3}x) + 2\sqrt{2n}\log 2n\,.$$

It follows that

$$\nu(x) - \nu(\frac{1}{2}x) \geq \left(\log 4 - \frac{\Delta}{3}\right) x - 2\sqrt{x}\log x - 2\log 4\,.$$

This immediately proves *Bertrand's Postulate*: $\nu(2x) - \nu(x) > 0$ (at least for x large). This also gives:

$$\begin{aligned} \nu(x) &\geq 2\left(\log 4 - \frac{\Delta}{3}\right) x - 2(2+\sqrt{2})\sqrt{x}\log x - 4\log^2 2\log x - 3\left(\log 4 - \frac{\Delta}{3}\right) \\ &\geq \end{aligned}$$

□

1.6. Chinese Remainder Theorem (18/9/09) [1, §2.3]

- Primes: The Euler product for the Riemann zeta-function and Euler's proof that there are infinitely many primes. The PNT. The idea of local-to-global.
- Statement; formulation as an isomorphism of finite rings.
- Proof by induction on number of factors.

Math 437/537: Problem set 2 (due 30/9/09)

Primes

1. Let $a,b \in \mathbb{Z}$ be positive and relatively prime. Show that ab is a perfect kth power iff both a and b are.

2. (Sum of divisors) For a positive integer n write $\sigma(n) = \sum_{d|n} d$ for the sum of its positive divisors (for example, $\sigma(6) = 1+2+3+6 = 12$).
   (a) Let p be prime. Show that $\sigma(p^r) = \frac{p^{r+1}-1}{p-1}$.
   (b) Let a,b be relatively prime. Show that $\sigma(ab) = \sigma(a)\sigma(b)$.

3. (Mersenne and Fermat primes)
   (a) Let $2^a - 1$ be prime. Show that a is prime.
   (b) Let $2^b + 1$ be prime. Show that b is a power of 2.

4. A positive integer n is called *deficient, perfect, or abundant* if $\sigma(n) < 2n$, $\sigma(n) = 2n$, or $\sigma(n) > 2n$ (for example, $6 = 3+2+1$ is perfect).
   (a) Show that 2^a is deficient for all $a \geq 1$.
   (b) Let m be odd, $a \geq 1$, and let $n = 2^a m$ be an even perfect number. Show that $2^{a+1} - 1 | m$. *Hint*: Use 2(b).
   (c) Writing $r = \frac{m}{2^{a+1}-1}$ show that $\left(2^{a+1}-1\right)(m+r) = 2n$. Conclude that the only positive divisors of m are r, m.
   (d) Show that every even perfect number is of the form $2^{p-1}(2^p - 1)$ where p is a prime such that $2^p - 1$ is also a prime.

5. For a prime p and integer n fine the exponent e so that $p^e \| n!$ (read: p^e divides $n!$ *exactly*; that is such that $p^e | n!$ but $p^{e+1} \not| n!$).

The Chinese Remainder Theorem

6. Call an integer n *squarefree* if it is not divisible by the square of a non-unit, that is if $d^2 | n$ implies $d | 1$.
   (a) Show that n is squarefree iff it is not divisible by the square of any prime.
   (b) Given $r \geq 1$ show that there exists $n \geq 1$ so that $\{n+j\}_{j=1}^{r}$ are all not squarefree. Conclude that there are arbitrarily large gaps between square-free numbers.

7. Find the smallest positive integer x such that $x \equiv 5\,(12)$, $x \equiv 2\,(5)$ and $x \equiv 4\,(7)$ all hold simultaneously.

8. Which integers x satisfy $2x \equiv 1\,(3)$, $3x \equiv 2\,(5)$, $4x \equiv 3\,(7)$, $7x \equiv 6\,(13)$ simultaneously?
   Hint: There is a simple solution!

9. For a non-zero integer n set $\phi(n) = |\{1 \leq d \leq |n| \mid (d,n) = 1\}|$ for the number of residue classes $\bmod n$ which are relatively prime to n. Let a,b be relatively prime. Show that $\phi(ab) = \phi(a)\phi(b)$.

Congruences

10. Let $(n,7)=1$. Show that $7|n^{12}-1$ directly (without using induction).

11. Let a,b be (separately) relatively prime to 91. Show that $a^{12}\equiv b^{12}\,(91)$.

12. (Divisibility tests I) For an integer n define $S_{k;10}(n)$ by the following procedure:
    - Write n in base 10
    - Divide the sequence of digits into blocks of length k, starting with the least significant digit (the last block may be shorter).
    - $S_{k;10}(n)$ is the sum of the numbers whose decimal representations are the blocks.

    (a) Show $S_{1;10}(n)\equiv n\,(9)$, and explain how to use this to test whether an integer n is divisible by 3.
    (b) Show $S_{6;10}(n)\equiv n\,(7)$, and explain how to use this to test whether an integer n is divisible by 7.

13. (General divisibility test) Given a base $b\geq 2$ and a number d relatively prime to b find k so that $S_{k;b}(n)\equiv n\,(d)$. Obtain a method to test whether numbers written in base b are divisible by d.

CHAPTER 2

The multiplicative group

2.1. Application: solving $x^2 \equiv -1\,(m)$ (21/9/09)

LEMMA 36. *Let p be an odd prime, $e \geq 1$. Then $x^2 \equiv 1\,(p^e)$ has exactly the two solutions $x \equiv \pm 1\,(p^e)$.*

PROOF. Since $(x+1, x-1) = (2, x+1)$, $p^e \mid (x-1)(x+1)$ implies $p^e \mid (x-1)$ or $p^e | (x+1)$. □

LEMMA 37. *The solutions to $x^2 \equiv 1\,(2^e)$ are: $\{\pm 1, 2^{e-1} \pm 1\}$ if $e \geq 3$, $\{\pm 1\}$ if $e = 2$, $\{1\}$ if $e = 1$.*

PROOF. The analysis above shows that if $x \not\equiv \pm 1$ then either $2^{e-1} | (x-1)$ and $2 | (x+1)$ or the reverse. □

COROLLARY 38. *$x^2 \equiv 1\,(m)$ has 2^a solutions, where $a = \omega(n) + \begin{cases} 1 & v_2(n) \geq 3 \\ 0 & v_2(n) = 2, 0. \\ -1 & v_2(n) = 1 \end{cases}$*

2.2. The Multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$

- (23/9/09) Euler function; Multiplicativity of Euler function via CRT.
- Order; divisibility; Euler generalization of Little Fermat.
- (25/9/09) Cyclic subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$ and primitive roots.
- Cannot have primitive root unless $m = p^e$ or $2p^e$ with p odd, or if $m = 4$. State that this is sufficient.
- Fermat's Little Theorem implies that$x^2 \equiv -1\,(p)$ has no solutions for $p \equiv 3\,(4)$. We will work on a converse.

2.3. $\mathbb{Z}/p\mathbb{Z}$ (30/09/10) [1, §2.7]

$\mathbb{Z}/p\mathbb{Z}$ is a field; $\mathbb{Z}/p\mathbb{Z}[x]$ is a PID; $x^p - x$ factors completely there. Conclude that any divisor factors completely there. In particular, $x^d - 1$ for $d | p-1$.

Primitive roots: if $q^e \| p-1$ then there are $q^e - q^{e-1}$ elements of order q^e. By CRT get element of order $p-1$, that is a primitive root.

$\left(\frac{-1}{p}\right)$ by studying elements of order 4.

Math 437/537: Problem set 3 (due 16/10/09)

Euler function

1. Find all solutions in positive integers to $\phi(x) = 24$.

2. For each $n \geq 1$ show that there are finitely many solutions to $\phi(x) = n$.

3. Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. For $m \in \mathbb{Z}_{\geq 1}$ let $N_f(m)$ denote the number of solutions in $\mathbb{Z}/m\mathbb{Z}$ to the congruence $f(x) \equiv 0\,(m)$. Let $\phi_f(m) = |\{a \in \mathbb{Z}/m\mathbb{Z} \mid (f(a), m) = 1\}|$.
   (a) Show that ϕ_f is multiplicative, that is that $\phi_f(nm) = \phi_f(n)\phi_f(m)$ whenever $(m,n) = 1$.
   (b) For p prime and $e \geq 1$ find $\phi_f(p^e)$ in terms of $\phi_f(p)$.
   (c) For p prime show that $\phi_f(p) + N_f(p) = p$.
   (d) Show that $\frac{\phi_f(n)}{n} = \prod_{p|n}\left(1 - \frac{N_f(p)}{p}\right)$ for all n.

Multiplicative groups

4. Let $m \geq 1$ and let $a, b \in (\mathbb{Z}/m\mathbb{Z})^\times$ have orders r, s respectively. Let t be the order of ab. Show:
$$\frac{rs}{(r,s)^2}\Big| t \qquad \text{and} \qquad t \Big| \frac{rs}{(r,s)}\,.$$

5. Let p be a prime. How many solutions are there to $x^4 - x^2 + 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$?
   Hint: Factor $x^{12} - 1$ in $\mathbb{Z}[x]$.

Primality Testing I - Carmichael numbers

We'd like to determine whether a given $m \in \mathbb{Z}_{\geq 1}$ is prime. For this we generate $a \in \mathbb{Z}/m\mathbb{Z}$ (represented as integers in the range $0 \leq m-1$) and test their multiplicative properties mod m.

6. Assume that our calculations produce some power a^k with $\left(a^k, m\right) > 1$ (perhaps $k = 1$!). Explain why this resolves the question about m.

We will therefore implicitly assume from now on that $(a,m) = 1$. Our first attempt will be to generate numbers $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ and check whether $a^{m-1} \equiv 1\,(m)$.

7. Show that if $(a, 561) = 1$ then $a^{560} \equiv 1\,(561)$ yet that 561 is composite.
   Hint: use the Chinese Remainder Theorem.

8. Let p be a prime and assume $p^2|m$. Show that $(\mathbb{Z}/m\mathbb{Z})^\times$ contains an element of order p, and conclude that there exists $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $a^{m-1} \not\equiv 1\,(m)$.

DEFINITION. Call a composite number m a *Carmichael number* if the statement of Fermat's little Theorem holds modulu m, that is if for any a relatively prime to m one has $a^{m-1} \equiv 1\,(m)$.

9. (Korselt's criterion) Show that m is a Carmichael number iff it is square-free, and for every $p|m$ one has $(p-1)|(m-1)$.

10. Find all Carmichael numbers of the form $3pq$ where $3 < p < q$ are primes.

Primality Testing II - the Miller-Rabin test.

From now on we assume that m an odd number and write $m-1=2^e n$ with n odd. Let $f \leq e-1$ be maximal such that there exists $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $x^{n2^f} = -1$. Write $s = n2^f$ and set

$$B = \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^\times \mid a^n \equiv 1\,(m) \text{ or } \exists 0 \leq j < e : a^{n2^j} \equiv -1\,(m) \right\},$$

$$B' = \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^\times \mid a^s \equiv \pm 1\,(m) \right\},$$

$$B'' = \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^\times \mid a^{m-1} \equiv 1\,(m) \right\}.$$

11. Show that $B \subset B' \subset B''$, and that B' and B'' are closed under multiplication.

12. Let m be prime. Show that $B = (\mathbb{Z}/m\mathbb{Z})^\times$.
Hint: If $a^n \neq 1$ let $b_j = a^{2^j n}$. Then $b_{j+1} = b_j^2$ and $b_e = 1$.

13. Assume that m is composite and that $B' = (\mathbb{Z}/m\mathbb{Z})^\times$.
    (a) Show that there exists relatively prime $m_1, m_2 > 2$ such that $m = m_1 m_2$.
    Hint: consider B''.
    (b) Let $x \in \mathbb{Z}$ satisfy $x^s \equiv -1\,(m)$. Show that there exists $y \in \mathbb{Z}$ such that $y^s \equiv -1\,(m_1)$ but $y^s \equiv 1\,(m_2)$ and conclude that B' is a proper subset.

14. Assume that m is composite. Show that $b \in (\mathbb{Z}/m\mathbb{Z})^\times \setminus B'$ implies $bB' \cap B' = \emptyset$ and conclude that $|B| \leq |B'| \leq \frac{1}{2}\left|(\mathbb{Z}/m\mathbb{Z})^\times\right|$.

ALGORITHM. *(Rabin) Input: an integer $m \geq 2$.*
(1) *If m is even, output "prime" if $m = 2$, "composite" otherwise and stop. If m is odd, continue.*
(2) *Repeat the following k times (k is fixed in advance):*
    (a) *Generate $a \in \{1, \ldots, m-1\}$, uniformly at random.*
    (b) *If $(a,m) > 1$, output "composite" and stop.*
    (c) *Check whether $a \in B$. If not, output "composite" and stop.*
(3) *Output "prime".*

15. (Primality testing is in BPP)
    (a) Show that if m is prime, the algorithm always output "prime".
    (b) Show that if m is composite, the algorithm outputs "s with probability at least $1 - \frac{1}{2^k}$.

OPTIONAL Find c so that the algorithm runs in time $O(k(\log_2 m)^c)$.
Hint: Given $1 \leq a \leq m-1$ efficiently calculate $a, a^2, a^4, a^8, a^{16}, \ldots$ and use that to calculate $a^n (\mod m)$ in time polynomial in $\log n$ and $\log m$.

REMARK. There exist infinitely many Carmichael numbers; see the paper of Alford, Granville and Pomerance, Annals of Math. (2) v. 140 (1994).

2.4. $\mathbb{Z}/p^k\mathbb{Z}$ (2/10/09) [1, §2.8]

- If g is a primitive root $\mod p$ and $g^{p-1} \equiv 1\,(p^2)$ then $(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + O(p^2) \equiv 1 - g^{p-2}p + O(p^2)$. Now g^{p-2} is not divisible by p so this isn't $1 \mod (p^2)$. If g is a primitive root mod p^k, $k \geq 2$, assume $g^{p^{k-2}(p-1)} = 1 + tp^{k-1}$ with $(t,p) = 1$. Raising to pth power we find

$$g^{p^{k-1}(p-1)} = 1 + tp^k + O(p^{k+1}),$$

that is g has order $p^k(p-1)$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$.
- Reformulation of proof: Set $U_r = \left\{ a \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \mid a \equiv 1\,(p^r) \right\}$, kernel of map to $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Then U_r is cyclic of order p^{k-r} (if $p = 2$ need $r \geq 2$). For this assume $p \geq 3, r \geq 1$ or $p = 2$ and $r \geq 2$, and let $\alpha \in U_r \setminus U_{r+1}$ so $\alpha = 1 + up^r$, $0 < u < p-1$. Then $\alpha^p = 1 + up^{r+1} + \sum_{k=2}^{p-1} \binom{p}{k} u^k p^{kr} + u^p p^{pr}$ or $\alpha^2 = 1 + u2^{r+1} + u^2 2^{2r}$. Now if p is odd then $pr \geq 3r \geq r+2$ and for $2 \leq k < p$ $kr \geq r+1$ while $p \mid \binom{p}{k}$. If $p = 2$, $2^{r+2} | 2^{2r}$ as long as $r \geq 2$. We conclude $\alpha^p \in U_{r+1} \setminus U_{r+2}$. Finally, choose $\alpha \in U_r \setminus U_{r+1}$. Then $\alpha^{p^{k-r-1}} \in U_{k-1} \setminus U_k$ so α has order p^{k-r}.
- When $p = 2$ no more to say. when p odd take primitive root $\beta \mod p$. Then some power β' of β has order $p-1$ modulu p^k and then $\alpha\beta'$ is a primitive root.

2.5. Diffie-Hellman (1976) & Rivest-Shamir-Adelman (1978)

- Need to share secrets without pre-shared secrets
- One-time-pad by courier
- Alice & Bob, Eve
- Based on functions which are easy to compute, hard to invert.
- We will rely on the functions $x \mapsto x^a$ and $a \mapsto x^a$ modulu m.

2.5.1. DH.

- Take a finite abelian group A and $g \in A$. Alice sends g^a, Bob sends g^b. Both compute g^{ab}.
- Most cases $A = (\mathbb{Z}/m\mathbb{Z})^\times$ but other groups used (e.g. Elliptic curves). Why not Zm?
- Best if g is an element of large order. Best if order is prime – if product of many small divisors then efficient heuristic algorithms work.
- Practical: let p be a prime such that $m = 2p+1$ is prime too. Then $\varphi(m) = 2p$, so any $g \in (\mathbb{Z}/m\mathbb{Z})^\times$ has order $2, p$ or $2p$. Best to use g of order p (otherwise can tell the lower bit of a depending on whether g^a is a square).
- Sophie Germaine; SG primes and application to FLT.

2.5.2. RSA.

- Full cryptographic scheme, including encryption, decryption and authentication (digital signatures).
- Asymmetric: Bob transmits to Alice.
- Alice:
  - Generates two large primes p, q and sets $m = pq$. She computes $\varphi(m) = (p-1)(q-1)$.

  - We will work in $(\mathbb{Z}/m\mathbb{Z})^\times$. Note that knowing both m and $\varphi(m)$ is equivalent to knowing p, q.
  - Chooses an exponent e and finds d so that $de \equiv 1\,(\varphi(m))$.
  - Publishes (m, e) ("public key"). Keeps (m, d) ("private key") secret.
- Algorithm
  - Bob wants to send a message $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.
  - He calculates $b = E(a) = a^e \pmod m$ and sends this to Alice.
  - Alice calculates $D(b) = b^d$. By Euler's Theorem $a^{ed} = a \cdot a^{ed-1} \equiv a\,(m)$ so $D(b) = D(E(a)) = a$.
- Note that $E(D(a)) = a$ as well. This allows Alice to securely sign messages:
  - Alice creates a message a she wants to send. She creates the pair $a' = (a, D_A(a))$.
  - Anyone can verify that it was Alice that created the message by verifying that $E_A(D_A(a)) = a$ (note that anyone can calculate E_A).
  - No-one can forge messages except by breaking the scheme.
  - Perhaps Alice sends the message securely, by sending Bob $E_B(a')$.
  - Alice can prove her identity this way by advertising $(a, D_A(a))$ for a random a.
  - Alice's public key may be stored by a central authority.

CHAPTER 3

Polynomial equations

3.1. Hensel's Lemma (7/10/09, 9/10/09) [1, §2.6]

EXAMPLE 39. $\sqrt{1+x}$ in $R[x]$. Set $f_0(x) = 1$.

- Try $f_1(x) = 1 + ax$. Then $f_1^2 = 1 + 2ax + a^2x^2 = 1 + 2ax + O(x^2)$ so try $a = \frac{1}{2}$.
- Try $f_2(x) = 1 + \frac{1}{2}x + bx^2$. Then $f_2(x)^2 = 1 + x + (2b + \frac{1}{4})x^2 + O(x^3)$ so try $b = -\frac{1}{8}$.
- Say $f_k(x)$ has degree k, $f_k^2(x) = 1 + x + O(x^{k+1})$. Try $f_{k+1}(x) = f_k(x) + a_{k+1}x^{k+1}$. Since

$$\left(f_k(x) + a_{k+1}x^{k+1}\right)^2 = f_k^2 + 2a_{k+1}x^{k+1} + O(x^{k+2})$$

  we can choose a_{k+1} to make $f_{k+1}^2 = 1 + x + O(x^{k+1})$ as long as 2 is invertible.

REMARK 40. Argument actually lives in $R[[x]]$ and its quotients $R[[x]]/(x^{k+1}) = R[x]/(x^{k+1})$.

Same phenomenon in $\mathbb{Z}/p^k\mathbb{Z}$.

DEFINITION 41. Let $f = \sum_{i=0}^n a_i x^i \in R[x]$. The *formal derivative* of f is the polynomial $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$.

LEMMA 42. *Let $f \in \mathbb{Z}[x]$. Then $f(x+h) = f(x) + hf'(x) + h^2Q(x,h)$ in $R[x,h]$.*

PROOF. Write the claim as $f(x+h) - f(x) - hf'(x) \in h^2R[x,h]$. This is clearly linear in f so enough to prove for $f(x) = x^n$, where $(x+h)^n - x^n = nhx^{n-1} + O(h^2)$ by the binomial theorem. □

LEMMA 43. *Let $f \in \mathbb{Z}[x]$ and let $a_k \in \mathbb{Z}$ be such that $f(a) \equiv 0\,(p^k)$ and $f'(a) \not\equiv 0\,(p)$. Then $\exists! b \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ such that $b \equiv a\,(p^k)$ and $f(b) \equiv 0\,(p^{k+1})$, given by $b = a - \frac{f(a)}{f'(a)}$.*

PROOF. We have $f(a+tp^k) = f(a) + tp^k f'(a) + O(p^{2k}) = p^k\left(\frac{f(a)}{p^k} + tf'(a)\right) + O(p^{k+1})$. Thus, $f(a+tp^k) \equiv 0\,(p^{k+1})$ iff $tf'(a) + \frac{f(a)}{p^k} \equiv 0\,(p)$. This clearly has the unique solution. In fact, if $u \in \mathbb{Z}$ is chosen such that $uf'(a) \equiv 1\,(p)$ it is clear we must take $b = a - uf(a)$. □

COROLLARY 44. *Let $f \in \mathbb{Z}[x]$, $a_1 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(a_1) = 0$, $f'(a_1) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Then for each $k \geq 1$ there is a unique $a_k \in \mathbb{Z}/p^k\mathbb{Z}$ so that $f(a_k) = 0$ and $a_k \equiv a_1\,(p)$.*

PROOF. Fix $u \in \mathbb{Z}$ so that $ua_1 \equiv 1\,(p)$, set $a_{k+1} = a_k - uf(a_k)$. Note that all the a_k are congruence modulu p so the same u works for all of them. □

REMARK 45. Two things:

(1) Note that this is similar Newton's method: $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$. In fact, choosing the inverse in $\mathbb{Z}/p^k\mathbb{Z}$ instead of $\mathbb{Z}/p\mathbb{Z}$ gives quadratic convergence.
(2) Note that the same proof would work if we replaced $\mathbb{Z}/p^k\mathbb{Z}$ with $F[y]/(y^k)$ for a field F.

What if f' vanishes too? This is an indication of a *multiple root*.

DEFINITION 46. Call $a \in \mathbb{Z}/p\mathbb{Z}$ such that $f(a) = 0$ a *regular root* if $f'(a) \neq 0$, a *singular root* if $f'(a) = 0$.

THEOREM 47. *(Hensel's Lemma) Let $f \in \mathbb{Z}[x]$. Let $a_1 \in \mathbb{Z}$ be such that $p^r \| f'(a_1)$ and $f(a_1) \equiv 0\,(p^{2r+1})$. Then for each k there exists $a_k \in \mathbb{Z}$, unique $\mod p^{r+k}$ such that $a_k \equiv a_1\,(p^{r+1})$ and $f(a_k) \equiv 0\,(p^{2r+k})$.*

PROOF. We note first that $f'(a+tp^k) \equiv f'(a)\,(p^k)$ so if $k > r$, $p^r \| f'(a+tp^k)$ no matter what t is. It follows that the same induction scheme will work: for some $k > r$ we will assume that $f(a) \equiv 0\,(p^{k+r})$ and produce $t \in \mathbb{Z}$, unique $\mod p$, so that $f(a+tp^k) \equiv 0\,(p^{k+1+r})$. Indeed, $f(a+tp^k) \equiv f(a) + tp^k f'(a)\,(p^{2k})$. Dividing by p^{k+r} (note that $p^{k+r} | p^{2k}$) we have

$$\frac{f(a+tp^k)}{p^{k+r}} \equiv \frac{f(a)}{p^{k+r}} + t\frac{f'(a)}{p^r}\,(p^{k-r}).$$

Since $k - r \geq 1$, we have $p^{k+1+r} \mid f(a+tp^k)$ iff $\frac{f(a)}{p^k} + t\frac{f'(a)}{p^r} \equiv 0\,(p)$. By assumption, $\frac{f'(a)}{p^r}$ is prime to p, so the congruence has a unique solution $\mod p$. □

EXAMPLE 48. $f(x) = x^2 + x + 7$.

- $\mod 3$ we are considering $x^2 + x + 1 = (x-1)^2$, so the unique root is $x = 1$ and it is singular. $f(1) = 3^2$ while $f'(1) = 3$. In fact, since $9 | f(1)$ we know that every $a \in \mathbb{Z}/9\mathbb{Z}$ such that $a \equiv 1\,(3)$ will be a root.
- $\mod 9$ we have $f(1) = 9$, $f(4) = 27$, $f(-2) = 9$.
- It follows that any root in $\mathbb{Z}/27\mathbb{Z}$ is congruent to 4 $\mod 9$. $f(4) = 27$, $f(13) = 189 = 27 \cdot 7$, $f(-5) = 27$. None is divisible by 81 so there are no zeroes in $\mathbb{Z}/81\mathbb{Z}$.
- By completing the square, if m is odd then there is a zero mod m iff -27 is a square $\mod m$. If $m | 27$ then $-27 \equiv 0\,(m)$ so it is a square, but after it is not since it is divisible by an odd power of 3.

EXAMPLE 49. $f(x) = x^2 + x + 223$.

- $\mod 3$ this is $x^2 + x + 1$ and has the unique root $x = 1$, also $f(1) = 225 = 9 \cdot 25$.
- $\mod 9$ we have $f(4) = 243 = 3^5$ and $f(-2) = 225 = 9 \cdot 25$.
- It follows that every zero $\mod 27$ is $\equiv 4\,(9)$. Since $f'(4) = 9 = 3^2$, it follows that for every $k \geq 3$ there is a unique solution in $\mathbb{Z}/p^k\mathbb{Z}$, congruence to 4
- $-891 = -81 * 11$ hence this is a square $\mod m$ iff -11 is a square $\mod m$. Indeed $-11 \equiv 1\,(3)$.

Math 437/537: Problem set 4 (due 28/10/09)

Some polynomials

1. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ be a polynomial with integer coefficients of degree $n \geq 1$, and let $r = \frac{p}{q} \in \mathbb{Q}$ be a rational number with $(p,q) = 1$. Assume that $f(r) = 0$.
   (a) Show that $p|a_0$ and $q|a_n$.
   (b) Conclude that if $a_n = 1$ (f is *monic*) then $r \in \mathbb{Z}$.

2. Let $g(x) = x^6 - 53x^4 + 680x^2 - 1156 = (x^2-2)(x^2-17)(x^2-34)$. Show that $g(x) = 0$ has solutions in the real numbers and in $\mathbb{Z}/m\mathbb{Z}$ for all m, but that $g(x) = 0$ has no solutions in the rational numbers.

DEFINITION. Call $f \in \mathbb{Z}[\underline{x}]$ *homogeneous of degree r* (or a *form*) if every monomial appearing in f has total degree r. Call $\underline{a} \in \mathbb{Z}^n$ *primitive* if $\gcd(a_1, \ldots, a_n) = 1$.

3. Let f be a form in n variables. Show that $V_f(\mathbb{Z}) = \bigcup_{d \geq 1} \left(dV'_f(\mathbb{Z}) \right)$ where $V'_f(\mathbb{Z})$ is the set of primitive solutions to the equations $f = 0$.

4. Find all integral solutions to the following equations (*Hint*: reduce mod m for suitably chosen m).
   (a) $x^2 + y^2 = 9z + 3$.
   (b) $x^2 + 2y^2 = 8z + 5$.
   (c) $x^2 + y^2 + z^2 = 2xyz$.
   (d) $x^4 + y^4 + z^4 = 5x^2yz$.
   (e) $x^4 + 2x^3 + 2x^2 + 2x + 5 = y^2$

5. (Rational points)
   (a) Let $f \in \mathbb{Q}[x,y]$ be a cubic and let $g \in \mathbb{Q}[x,y]$ be linear and non-constant. Obtain a correspondence between $V_f(\mathbb{Q}) \cap V_g(\mathbb{Q})$ and the roots of a polynomial of degree at most 3 with rational coefficient, and conclude that this set, if finite, has size at most 3.
   OPTIONAL Explain why the set cannot have size 2, if we count zeroes with multiplicity and include points at infinity.
   From now on let $f(x,y) = x^3 + 2x^2 - y^2$. We will find $V_f(\mathbb{Q}) \subset \mathbb{Q}^2$.
   (b) Let g be a linear polynomial so that $(0,0) \in V_g(\mathbb{Q})$. Show that $V_f(\mathbb{Q}) \cap V_g(\mathbb{Q})$ contains at most one more point.
   (c) Find all $\mathbb{Q}$-rational points on V_f.
   (d) Given $\varepsilon > 0$, show how to find a rational point $(x,y) \in V_f(\mathbb{Q})$ with $0 < |x|, |y| < \varepsilon$.
   (e) Exhibit specific $x, y \in \mathbb{Q}$ such that $y^2 = x^3 + 2x^2$ and $0 < |x|, |y| < \frac{1}{1000}$.

Using $\mathbb{Z}[i]$

6. (The issue at 2)
   (a) Let $w \in \mathbb{Z}[i]$ divide 2. Show that w is associate to one of $1, \pi, \pi^2$ where $\pi = 1 + i$.
   (b) Let $x, y \in \mathbb{Z}$ be relatively prime, and let $z = x + iy \in \mathbb{Z}[i]$. Show that $(z, \bar{z})$ divides 2 in $\mathbb{Z}[i]$. Conclude that $(z, \bar{z}) = \pi$ if x, y are both odd, $(z, \bar{z}) = 1$ otherwise.

(c) Now take any $x,y \in \mathbb{Z}$. Show that $(x+iy, x-iy) = (x,y) \cdot \begin{cases} \pi & \frac{x}{(x,y)}, \frac{y}{(x,y)} \text{ both odd} \\ 1 & \text{otherwise} \end{cases}$.

7. Let $x,y \in \mathbb{Z}$ satisfy $y^2 = x^3 - 1$.
   (a) Show that y is even and x is odd.
   Hint: reduce the equation modulu 4.
   (b) Let $z = 1+iy \in \mathbb{Z}[i]$. Show that $z\bar{z}$ is a cube in $\mathbb{Z}[i]$ and that $(z,\bar{z}) = 1$ there. Conclude that there exists $w \in \mathbb{Z}[i]$ and $\varepsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ such that $z = \varepsilon \cdot w^3$.
   (c) Examining the real and imaginary parts of the resulting identity, show that $x = 1$, $y = 0$ is the only solution.

8. Let $(x,y,z) \in \mathbb{Z}^3$ be primitive and satisfy $x^2 + y^2 = z^2$.
   (a) Show that x,y have different parities. WLG we'll assume that x is odd, y is even.
   (b) Show that $x+iy \in \mathbb{Z}[i]$ has the form $\varepsilon(m+in)^2$ for some relatively prime $m,n \in \mathbb{Z}$ and $\varepsilon \in \mathbb{Z}[i]^\times$.
   (c) Conclude that $(x,y,z) = \left(m^2 - n^2, 2mn, m^2 + n^2\right)$.
   - Note how the choice of root of unity corresponds to the choice of which of x,y is even.

Sums of two squares

9. Let $r_2(n) = \#\left\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 = n\right\}$ and set $s(n) = \frac{1}{4} r_2(n)$.
   (a) Show that $s(n)$ is integral and multiplicative.
   Hint: Adapt problem 6(a) from PS1 to $\mathbb{Z}[i]$.
   (b) For $k \geq 1$, and primes $p \equiv 1\,(4)$ and $q \equiv 3\,(4)$ show that $s(2^k) = 1$, $s(p^k) = k+1$, $s(q^k) = \begin{cases} 1 & k \equiv 0\,(2) \\ 0 & k \equiv 1\,(2) \end{cases}$.
   (c) Find the smallest integer n so that $r_2(n) = 60$.

10. Define a function $\chi_4 \colon \mathbb{Z}_{\geq 1} \to \{0, \pm 1\}$ by setting $\chi_4(n) = \begin{cases} 1 & n \equiv 1\,(4) \\ -1 & n \equiv 3\,(4) \\ 0 & 2|n \end{cases}$.
    (a) Show that $\chi_4(ab) = \chi_4(a)\chi_4(b)$ for all $a,b \in \mathbb{Z}$.
    (b) Show that $n \mapsto \sum_{d|n} \chi_4(d)$ is multiplicative.
    (c) show that $s(n) = \sum_{d|n} \chi_4(d)$ for prime powers n.
    (d) Show that $r_2(n) = 4\sum_{d|n} \chi_4(d)$ for all n.

Some arithmetic

11. The most recently discovered perfect number is $N = 2^{p-1}(2^p - 1)$, where $p = 42,643,801$. Determine how many digits N has, and find the first three digits (on the left) and the last three digits (on the right). You may use the equivalent of an abacus (e.g. a simple electronic calculator) to do the arithmetic, but not the equivalent of a general-purpose computer – for example do not evaluate N directly!

Roots of unity

Let $e(x) = e^{2\pi ix}$. For an integer m Let $\zeta_m = e(\frac{1}{m})$, $\zeta_m^k = e\left(\frac{k}{m}\right)$. Let $\mu_m = \left\{\zeta_m^k\right\}_{k\in\mathbb{Z}} \subset \mathbb{C}$.

12. Show that μ_m is the set of solutions to $z^m = 1$ in $\mathbb{C}$, and that it is closed under multiplication. Show that the map $k \mapsto \zeta_m^k$ induces a bijection $\mathbb{Z}/m\mathbb{Z} \to \mu_m$ mapping addition to multiplication. Fixing k, show that $\mu_m = \left\{\zeta_m^{kj}\right\}_{j\in\mathbb{Z}}$ iff $(k,m) = 1$. In that case we call ζ_m^k a *primitive* root of unity of order m.

13. Given $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ and $j \in \mathbb{Z}/m\mathbb{Z}$ set $\hat{f}(k) = \sum_{j(m)} f(j)\zeta_m^{-jk} = \sum_{a(m)} f(a)e(\frac{ak}{m})$. We call $\hat{f}$ the *Discrete Fourier Transform* of f.
    (a) Show that $\sum_{k(m)} \zeta_m^{kj} = m\delta_{j,0}$.
    (b) Show that $\hat{\hat{f}}(k) = f(-k)$ ("Fourier inversion").
    (c) Show that $\sum_{j(m)} |f(j)|^2 = \frac{1}{m}\sum_{k(m)} \left|\hat{f}(k)\right|^2$ ("Parseval's identity").

3.2. Various equations (12-16/10)

3.2.1. For which primes p are there $a,b \in \mathbb{Z}$ so that $a^2+b^2=p$?

(1) $1^2+1^2=2$, so from now on assume p is odd.
(2) If $p \mid a^2+b^2$ and a,b are not divisible by p then -1 is a square mod p hence $p \equiv 1\,(4)$.
(3) If $p \equiv 1\,(4)$ then there exists a such that $a^2 \equiv -1\,(p)$. It follows that $p|(1+ia)(1-ia)$ in $\mathbb{Z}[i]$. Since p divides neither, it is not a prime. Say $p=zw$ with $z,w \in \mathbb{Z}[i]$ non-units. Then $p^2=Np=NzNw$ since $Nz,Nw \neq 1$ it follows that $Nz=p$.
(4) Alternative: Let z be a prime divisor of p. By symmetry the same holds for $\bar{z}$, and they are not associates: $\frac{z}{\bar{z}}=\frac{z^2}{N(z)}=\frac{x^2-y^2}{x^2+y^2}+\frac{2xy}{x^2+y^2}i$, and $\frac{x^2-y^2}{x^2+y^2} \in \mathbb{Z}$ only if $x=0$ or $y=0$ or $x^2=y^2$. Neither of $z,\bar{z}$ is associate to an element of $\mathbb{Z}$ since p is prime there, neither is associate to $1+i$ since $(1\pm i)^2=\pm 2i$ would divide p^2 but p is odd. It follows that $z\bar{z}|p$ in $\mathbb{Z}[i]$ so in $\mathbb{Z}$. It follows that $Nz|p$. Since it's not 1 it equals p and we are done.

THEOREM 50. *(Fermat) The equation $x^2+y^2=p$ has a solution iff $p=2$ or $p \equiv 1\,(4)$.*

Alternative proof:

Let m be minimal so that there exist x,y with $x^2+y^2=mp$. $m<p$ since we have $0<a<p$ with $1+a^2 \equiv 0\,(p)$. Assuming $m>1$ take $a \equiv x\,(m)$ and $b \equiv y\,(m)$ with $|a|,|b| \leq \frac{m}{2}$. We then have:

$$ay-bx \equiv xy-yx \equiv 0\,(m)$$

and

$$ax+by \equiv x^2+y^2 \equiv 0\,(m).$$

Consider now

$$\left(\frac{ay-bx}{m}\right)^2+\left(\frac{ax+by}{m}\right)^2=\frac{a^2y^2+b^2x^2+a^2x^2+b^2y^2}{m^2}=\left(\frac{a^2+b^2}{m}\right)\left(\frac{x^2+y^2}{m}\right).$$

We have $\frac{x^2+y^2}{m}=p$ and $m'=\frac{a^2+b^2}{m} \leq \frac{1}{4}m+\frac{1}{4}m=\frac{1}{2}m<m$. It follows that $m'p$ is a sum of two squares with $m'<m$, a contradiction.

3.2.2. For which n are there $a,b \in \mathbb{Z}$ so that $a^2+b^2=n$?

LEMMA 51. *$n=2^e\prod_i p_i^{f_i}\prod q_j^{2g_j}$ with $p_i \equiv 1\,(4)$ and $q_i \equiv 3\,(4)$ is sufficient.*

PROOF. Enough to check for 2, p_i, and q_j^2. □

THEOREM 52. *(Fermat) The condition is necessary and sufficient.*

PROOF. Let $a^2+b^2=n$ and let $q \equiv 3\,(4)$ divide n. Assume that $q \nmid a$ let $\bar{a}$ be an inverse to a modulu q. This would imply $(\bar{a}b)^2 \equiv -1\,(q)$, contradicting $q \equiv 3\,(4)$. Thus $q|a$, $q|b$ which means $q^2|n$ and $\left(\frac{a}{q}\right)^2+\left(\frac{b}{q}\right)^2=\frac{n}{q^2}$. We are now done by induction. □

3.2.3. Solve $y^2=x^3+1$ in $\mathbb{Z}$.

3.2.4. Solve $y^2 = x^3 - 1$ in $\mathbb{Z}$. Assume first that y is odd. Then $y^2 + 1 \equiv 2\,(4)$ while x^3 is divisible by 8 since x is even. It follows that y is even. Next, any common divisor of $1+iy$, $1-iy$ in $\mathbb{Z}[i]$ divides 2. But $\frac{1+iy}{1+i} = \frac{(1+iy)(1-i)}{2} = \frac{1+y+(y-1)i}{2}$ which is not integral if y is even. By unique factorization we see that $1+iy$ is associate to a cube. Say

$$1 + iy = \varepsilon(a+bi)^3\,.$$

Taking real parts we find either:

$$1 = \pm(a^3 - 3ab^2)$$

or

$$1 = \pm(b^3 - 3a^2b)\,,$$

which we treat symmetrically. In the first case we have $a = \pm 1$ (it divides 1) and $3b^2 - 1 = \pm 1$. This is only possible if $b = 0$. So we have $1 + iy = \pm 1$, that is $y = 0$.

THEOREM 53. *The only solution to $y^2 = x^3 - 1$ in $\mathbb{Z}^2$ is $(1,0)$.*

EXERCISE 54. Consider $y^2 = x^p - b^2$ where p is an odd prime and b is odd.
Again y must be even due to $\mathbb{Z}/4\mathbb{Z}$.

3.2.5. Solve $x^2 + y^2 = z^2$ in $\mathbb{Z}$. Enough to consider positive primitive solutions. Say x, z odd and y even. Then

$$\frac{y^2}{4} = \frac{z-x}{2} \cdot \frac{z+x}{2}$$

and the two are relatively prime. Thus there exist relatively prime $m, n > 0$ so that $z - x = 2m^2$, $z + x = 2n^2$. Then $z = m^2 + n^2$, $x = m^2 - n^2$, $y = 2mn$. Conversely, if $(m,n) = 1$ then x, y, z is a primitive solution.

3.2.6. Solve $x^4 - y^4 = z^2$ in $\mathbb{Z}$. If $p|(x,y,z)$ then $p^4|z^2$ so enough to consider primitive solutions.

If x, y are odd then z is even and $x^4 = z^2 + y^4$ so there exist m, n so that $z = 2mn$, $y^2 = m^2 - n^2$, $x^2 = m^2 + n^2$ so $x^2y^2 = m^4 - n^4$. Furthermore, $m < x$ – contradiction. If x, y have different parities there exist m, n so that $m^2 = x^2 + y^2$ and $n^2 = x^2 - y^2$. Let $u = \frac{m-n}{2}$, $v = \frac{m+n}{2}$. Then u, v are relatively prime and $2uv = y^2$. Say v is even (so $\frac{v}{2}$ and u are squares). Then $u^2 + v^2 = x^2$ from there exist k, l so that $u = k^2 - l^2$, $v = 2kl$, $x = k^2 + l^2$. From $\frac{v}{2} = kl$ conclude that k, l are squares and then $u = k^2 - l^2$ is a smaller solution.

CHAPTER 4

Quadratic reciprocity

4.1. Quadratic Residues (19/10)

The multiplicative group; power residues. Residues and non-residues; number of residues. Legendre symbol.

THEOREM 55. *(Euler) Let p be an odd prime, and let $a,b \in \mathbb{Z}$. Then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (p)$. In particular:*

(1) *If $a \equiv b\,(p)$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

4.2. The Quadratic character of 2 (19/10)

Given a, would like to find the p so that $\left(\frac{a}{p}\right) = 1$. For $a = -1$ know that $\left(\frac{a}{p}\right)$ depends on residue class of p mod 4. We now calculate $\left(\frac{2}{p}\right)$.

THEOREM 56. *Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

PROOF. Would like to evaluate $2^{\frac{p-1}{2}}$. For this we need a good square root of 2, and notice that $(1+i)^2 = 2i$ in $\mathbb{Z}[i]$. It follows that

$$(1+i)^{p-1} = (2i)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} i^{\frac{p-1}{2}}$$

so

$$\left(\frac{2}{p}\right) \equiv i^{-\frac{p-1}{2}} (1+i)^{p-1}\,(p)\,.$$

Multiplying by $(1+i)$ and using $(a+b)^p \equiv a^p + b^p$ we have:

$$(1+i)\left(\frac{2}{p}\right) \equiv i^{-\frac{p-1}{2}} \left(1+i^p\right)\,(p)\,.$$

Multiplying by $(1-i)$ we have:

$$2\left(\frac{2}{p}\right) \equiv i^{-\frac{p-1}{2}} (1-i)(1+i^p)\,(p)\,.$$

We now evaluate the RHS, depending on the residue class of p mod 8.

$p \equiv 1\,(8)$ Then $\frac{p-1}{2} \equiv 0\,(4)$ and $p \equiv 1\,(4)$ so the RHS is $(1-i)(1+i) = 2$.

$p \equiv 3\,(8)$ Then $\frac{p-1}{2} \equiv 1\,(4)$ and $p \equiv 3\,(4)$ so the RHS is $(-i)(1-i)^2 = -2$.

$p \equiv 5\,(8)$ Then $\frac{p-1}{2} \equiv 2\,(4)$ and $p \equiv 1\,(4)$ so the RHS is $(-1)(1-i)(1+i) = -2$.
$p \equiv 7\,(8)$ Then $\frac{p-1}{2} \equiv 3\,(4)$ and $p \equiv 3\,(4)$ so the RHS is $(i)(1-i)^2 = 2$.
Since 2 is invertible mod p we conclude

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}\,(p)$$

where the congruence is in $\mathbb{Z}[i]$. Since both sides are ordinary integers it follows that $\frac{\left(\frac{2}{p}\right)-(-1)^{\frac{p^2-1}{8}}}{p} \in \mathbb{Z}[i] \cap \mathbb{Q} = \mathbb{Z}$. It follows that the congruence holds in $\mathbb{Z}$ and since both sides are ± 1 we must have equality. □

4.3. The Gauss sum (21/10)

DEFINITION 57. A *Dirichlet character* mod m is a map $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ zero-extended to $\mathbb{Z}/m\mathbb{Z}$ and pulled back to $\mathbb{Z}$.

Write χ_0 for the *principal character* $\chi_0(a) = \begin{cases} 1 & (a,m) = 1 \\ 0 & (a,m) > 1 \end{cases}$. Write ε for the *constant function* $\varepsilon(n) = 1$.

Let χ be a Dirichlet character mod p, let $b \in \mathbb{Z}/p\mathbb{Z}$. The *Gauss sum* is the Fourier transform

$$G(\chi;b) = \sum_{a(p)} \chi(a)\zeta_p^{ab} = \sum_{a(p)} \chi(a) e(\frac{ab}{p})$$
$$G(\chi) = G(\chi;1)\,.$$

For $r \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have:

$$G(\chi;rb) = \sum_{a(p)} \chi(a)\zeta_p^{arb} = \chi(r)^{-1} \sum_{a(p)} \chi(ar)\zeta_m^{arb} = \chi(r)^{-1} G(\chi;b)\,.$$

LEMMA 58. *Let p be prime, χ a non-trivial character.*
(1) $G(\varepsilon;0) = p$; $G(\chi;0) = 0$.
(2) $G(\varepsilon) = 0$; $|G(\chi)|^2 = p$.
(3) $G(\chi)G(\bar{\chi}) = \chi(-1)p$.

PROOF. $G(\varepsilon;0) = \sum_{a(p)} 1 = p$. We also have $G(\chi;0) = \chi(r)^{-1}G(\chi;0)$ for any r. Taking r so that $\chi(r) \neq 1$ shows $G(\chi;0) = \sum_{a(p)} \chi(a) = 0$.

Next, $\sum_{a(p)} \zeta_p^{ab} = \sum_{a=0}^{p-1} \left(\zeta_p^b\right)^a = \begin{cases} p & b = 0 \\ 0 & b \neq 0 \end{cases}$ by the formula for the geometric sum.

$$|G(\chi)|^2 = \sum_{a,b(p)} \chi(ab^{-1})\zeta_p^{a-b} = \sum_b{}' \sum_c{}' \chi(c)\zeta_p^{b(1-c)} = \sum_c{}' \chi(c) \sum_b{}' \zeta_p^{b(1-c)} = p\sum_c{}' \chi(c)\,[\delta_{1,c} - 1] = p\chi(1) - p\sum_{c\neq 0} \chi(c)$$

Also,

$$\overline{G(\chi;b)} = G(\bar{\chi};-b) = \chi^{-1}(-1)G(\bar{\chi};b)\,.$$

It follows that

$$G(\chi;b)G(\bar{\chi};b) = \chi(-1)\,|G(\chi;b)|^2 = p\chi(-1)$$

if $b \neq 0$. □

4.4. Quadratic reciprocity (23-26/10)

4.4.1. The law of quadratic reciprocity (23/10).

THEOREM 59. *(Quadratic reciprocity; Gauss) Let p,q be odd primes. Then*

(1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

(2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(3) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

PROOF. We have already seen (1),(2).

Let $\chi(a) = \left(\frac{a}{p}\right)$ be the quadratic character $\mod p$. Then $\chi = \bar{\chi}$ so $G(\chi)^2 = \chi(-1)p = (-1)^{\frac{p-1}{2}}p$. We will now do some calculations in the ring $\mathbb{Z}[\zeta_p] = \left\{\sum_{j=0}^{p-1} a_j \zeta_p^j \mid a_j \in \mathbb{Z}\right\}$, starting by the observation that $G(\chi) \in \mathbb{Z}[\zeta_p]$ since χ takes integral values. We evaluate $G(\chi)^{q+1}$ modulu q in two different ways. First,

$$G(\chi)^{q+1} = \left(G(\chi)^2\right)^{\frac{q+1}{2}} = G(\chi)^2(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}G(\chi)^2\left(\frac{p}{q}\right)(q).$$

Secondly,

$$\begin{aligned} G(\chi)^{q+1} &= G(\chi)G(\chi)^q \\ &\equiv G(\chi)\sum_{a(p)}(\chi(a))^q\,\zeta_p^{qa}\,(q) \\ &= G(\chi)G(\chi^q;q) \\ &= G(\chi)G(\chi;q) \\ &= \chi(q)G(\chi)^2, \end{aligned}$$

since $\chi = \chi^q = \chi^{-1}$. Comparing both results we find:

$$\chi(q)G(\chi)^2 \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)G(\chi)^2\,(q),$$

where the congruence is in $\mathbb{Z}[\zeta_\rho]$. Since $G(\chi)^2$ is invertible mod q and $\left(\frac{p}{q}\right) \in \{\pm 1\}$, this implies

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\,(q).$$

The equality of both sides now follows from the following Lemma. □

LEMMA 60. *Let $G \subset \mathbb{C}$ be finite and contain* 1*, and assume that $R = \mathbb{Z}[G] = \left\{\sum_{g\in G} a_g g \mid a_g \in \mathbb{Z}\right\} \subset \mathbb{C}$ is closed under multiplication. Then $R \cap \mathbb{Q} = \mathbb{Z}$.*

PROOF. Say $|G| = n$. Given $z \in R$ and $h \in G$ we have $zh \in R$ so there exist $a_{g,h} \in \mathbb{Z}$ so that $zh = \sum_g a_{g,h}g$. Let $A \in M_n(\mathbb{Z})$ be the matrix with entries $a_{g,h}$, and let $\underline{v} \in \mathbb{C}^G$ be the vector $v_g = g$. We have shown $(zI - A)\,\underline{v} = \underline{0}$. It follows that z is a zero of the characteristic polynomial $p_A(x) = \det(xI - A) \in \mathbb{Z}[x]$. Since $p_A(x)$ is monic its rational zeroes are all integral. □

EXAMPLE 61. $\left(\frac{-42}{61}\right)=\left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)=(-1)^{30}(-1)^{\frac{60^2+2\cdot 60}{8}}\left(\frac{61}{3}\right)\left(\frac{61}{7}\right)=(1)(-1)^{15}\left(\frac{1}{3}\right)\left(\frac{5}{7}\right)=-\left(\frac{7}{5}\right)=-\left(\frac{2}{5}\right)=-(-1)^{\frac{24}{8}}=1$. Also, $\left(\frac{-42}{61}\right)=\left(\frac{19}{61}\right)=\left(\frac{61}{19}\right)=\left(\frac{4}{19}\right)=1$.

4.4.2. The Jacobi symbol (26/10). Calculations above required factoring.

DEFINITION 62. Let $Q>1$ be odd, say $Q=\prod_j q_j$ with q_j primes (not necc distinct). For $P\in\mathbb{Z}$ set

$$\left(\frac{P}{Q}\right)\stackrel{\text{def}}{=}\prod_j\left(\frac{P}{q_j}\right).$$

LEMMA 63. *(Jacobi symbol) Let $P,P'\in\mathbb{Z}$ and let Q,Q' be odd and positive. Then*

(1) *If $P\equiv P'\,(Q)$ then $\left(\frac{P}{Q}\right)=\left(\frac{P'}{Q}\right)$.*

(2) $\left(\frac{PP'}{Q}\right)=\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right)$ *and* $\left(\frac{P}{QQ'}\right)=\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right)$.

THEOREM 64. *Let P,Q be odd and positive. Then*

(1) $\left(\frac{-1}{Q}\right)=(-1)^{\frac{Q-1}{2}}$.

(2) $\left(\frac{2}{Q}\right)=(-1)^{\frac{Q^2-1}{8}}$.

(3) $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$.

PROOF. These follow immediately from the corresponding properties of the Legendre symbol via the congruences (easily established by induction)

$$\sum_j\frac{q_j-1}{2}\equiv\frac{\prod_j q_j-1}{2}\,(2)$$

$$\sum_j\frac{q_j^2-1}{8}\equiv\frac{\prod_j q_j^2-1}{8}\,(2)$$

$$\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}\equiv\frac{\prod_i p_i-1}{2}\frac{\prod_j p_j-1}{2}\,(2)$$

where p_i,q_j are positive and odd. □

4.5. Jacobi sums (28-30/10)

In this section we use ε rather than χ_0 as the principal character.

4.5.1. A quadratic form. Write $N(x^2+y^2=1)$ for the number of solutions in $\mathbb{F}_p$. Noting that $N(x^2=a)=1+\left(\frac{a}{p}\right)$ we have:

$$N(x^2+y^2=1)=\sum_{a+b=1}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right)=\sum_{a+b=1}\left(1+\chi(a)+\chi(b)+\chi(ab)\right).$$

Here $\chi(a)=\left(\frac{a}{p}\right)$. Now $\sum_a\chi(a)=1$ and

$$\sum_{a+b=1}\chi(ab)=\sum_a\chi(a(1-a))=\sum_{a\neq 1}\chi((1-a)^2)\chi(\frac{a}{1-a})=\sum_{a\neq 1}\chi\left(\frac{a}{1-a}\right)=\sum_{c\neq -1}\chi(c)=-\chi(-1)$$

since $c=\frac{a}{1-a}$ is inverse to $a=\frac{c}{1+c}$. It follows that

$$N(x^2+y^2=1)=p-(-1)^{\frac{p-1}{2}}$$

which we interpret as a main term and an error term.

4.5.2. A cubic form. Let p be prime. Then $x^l\equiv a\,(p)$ has either zero or $d=(l,p-1)$ solutions, depending on whether a is a dth power or not.

LEMMA 65. *Let p be prime. Then there are $p-1$ characters mod p and $N(x^l\equiv a)=\sum_{\chi^d=\varepsilon}\chi(a)$.*

PROOF. Let g be a primitive root mod p. Then characters are determined by the value $\chi(g)$. Since $g^{p-1}\equiv 1\,(p)$ we have $\chi(g)^{p-1}=\chi(1)=1$. Thus $\chi(g)\in\mu_{p-1}$. Conversely, if $\zeta\in\mu_{p-1}$ set $\chi(g^r)=\zeta^r$. This is well-defined since if $g^r\equiv g^s\,(p)$ then $(p-1)|r-s$ so $\zeta^{r-s}=\left(\zeta^{p-1}\right)^{\frac{r-s}{p-1}}=1$ and $\zeta^r=\zeta^s$.

Next, if $a=0$ then $N(x^l\equiv a)=1$ and $\chi(a)=0$ for all characters except for ε. The proof for $a\neq 0$ is left as an exercise. □

THEOREM 66. *If $p\equiv 2\,(3)$, $N(x^3+y^3=1)=p$. If $p\equiv 1\,(3)$ then*

$$\left|N(x^3+y^3=1)-(p-2)\right|\leq 2\sqrt{p}$$

PROOF. If $p\equiv 2\,(3)$ then the map $x\mapsto x^3$ is invertible, and $N(x^3+y^3=1)=N(x+y=1)=p$. If $p\equiv 1\,(3)$, we have:

$$N(x^3+y^3=1)=\sum_{a+b=1}N(x^3=a)N(y^3=b)=\sum_{i,j=0}^{2}\chi^i(a)\chi^j(b)\,.$$

The $0,0$ summand is p. The $0,j$ and $i,0$ summands vanish, since $\sum_a\chi(a)=\sum_a\chi^2(a)=0$. We thus have

$$N(x^3+y^3=1)=p+2\sum_{a+b=1}\chi(a)\bar{\chi}(b)+\sum_{a+b=1}\chi(a)\chi(b)+\sum_{a+b=1}\bar{\chi}(a)\bar{\chi}(b)\,.$$

Next, $\sum_{a+b=1}\chi(a)\bar{\chi}(b)=\sum_{a\neq 1}\chi\left(\frac{a}{1-a}\right)=\sum_{c\neq -1}\chi(c)=-\chi(-1)=-\chi(-1)=-1$ since $(-1)^3=(-1)$. Finally,

$$\begin{aligned}
G(\chi)^2 &= \sum_{a,b}\chi(a)\chi(b)\zeta_p^{a+b}\\
&= \sum_{t\,(p)}\sum_{a+b=t}\chi(a)\chi(b)\zeta_p^t\\
&= \sum_a\chi(a)\chi(-a)+\sum_{t\neq 0}\chi(t)^2\zeta_p^t\sum_{a+b=t}\chi(\frac{a}{t})\chi\left(\frac{b}{t}\right)\\
&= \chi(-1)\sum_a\chi^2(a)+G(\chi^2)\sum_{a+b=1}\chi(a)\chi(b)\,.
\end{aligned}$$

It follows that

$$\sum_{a+b=1}\chi(a)\chi(b)=\frac{G(\chi)^2}{G(\chi^2)}\,.$$

In particular, $\left|\sum_{a+b=1}\chi(a)\chi(b)\right|=\sqrt{p}$. □

DEFINITION 67. Let $\chi_1,\dots,\chi_r$ be Dirichlet characters mod p. Set

$$J_0(\chi_1,\dots,\chi_r)=\sum_{\sum_i a_i=0}\prod_i\chi_i(a_i)$$

$$J(\chi_1,\dots,\chi_r)=\sum_{\sum_i a_i=1}\prod_i\chi_i(a_i)\,.$$

PROPOSITION 68. *Let $\chi,\lambda\neq\varepsilon$ so that $\chi\lambda\neq\varepsilon$. Then*

(1) $J_0(\varepsilon,\varepsilon)=J(\varepsilon,\varepsilon)=p$.
(2) $J_0(\chi,\varepsilon)=J(\chi,\varepsilon)=0$.
(3) $J_0(\chi,\chi^{-1})=\chi(-1)(p-1)$ *while* $J(\chi,\chi^{-1})=-\chi(-1)$.
(4) $J_0(\chi,\lambda)=0$ *while* $J(\chi,\lambda)=\frac{G(\chi)G(\lambda)}{G(\chi\lambda)}$ *so* $|J(\chi,\lambda)|=\sqrt{p}$.

PROOF. (1) is clear, (2) follows from $\sum_a\chi(a)=0$. For (3) note that $J_0(\chi,\chi^{-1})=\sum_a\chi(a)\chi^{-1}(-a)=\chi(-1)\sum_{a\neq0}\chi(a)\chi^{-1}(a)$ while $J(\chi,\chi^{-1})=\sum_{a\neq1}\chi\left(\frac{a}{1-a}\right)=\sum_{c\neq-1}\chi(c)=-\chi(-1)$. That $J_0(\chi,\lambda)=\lambda(-1)\sum_a(\chi\lambda)(a)=0$ is easy. Finally, we have:

$$\begin{aligned}G(\chi)G(\lambda) &= \sum_{a,b}\chi(a)\lambda(b)\zeta_p^{a+b}\\ &= \sum_{t(p)}\sum_{a+b=t}\chi(a)\lambda(b)\zeta_p^t\\ &= \sum_a\chi(a)\lambda(-a)+\sum_{t\neq0}(\chi\lambda)(t)\zeta_p^t\sum_{a+b=t}\chi(\frac{a}{t})\lambda\left(\frac{b}{t}\right)\\ &= 0+G(\chi\lambda)J(\chi,\lambda)\,.\end{aligned}$$

Since $|G(\chi\lambda)|=\sqrt{p}\neq0$ we are done. □

COROLLARY 69. *If $p\equiv1\,(4)$ then $p=a^2+b^2$ for some a,b. If $p\equiv1\,(3)$ then $p=a^2-ab+b^2$ for some $a,b\in\mathbb{Z}$.*

PROOF. Let χ be a character of order 4 in the first case, of 3 in the second. Then $\chi,\chi^2\neq\varepsilon$ and $J(\chi,\chi)\in\mathbb{Z}[i]$ in the first case, $J(\chi,\chi)\in\mathbb{Z}[\omega]$ in the second. Since $|J(\chi,\chi)|^2=p$ we are done (note that $(a+b\omega)(a+b\bar{\omega})=a^2+b^2+ab(\omega+\omega^2)=a^2-ab+b^2$). □

THEOREM 70. *Let $\chi_1,\dots,\chi_r\neq\varepsilon$ so $\rho=\prod_{i=1}^{r-1}\chi_i\neq\varepsilon$ and let $\lambda=\prod_{i=1}^r\chi_i$.*

(1) $J_0(\varepsilon,\dots,\varepsilon)=J(\varepsilon,\dots,\varepsilon)=p^{r-1}$.
(2) $J_0(\chi_1,\dots,\chi_s,\varepsilon,\dots,\varepsilon)=J_1(\chi_1,\dots,\chi_s,\varepsilon,\dots,\varepsilon)=0$ *where* $1\leq s\leq r-1$.
(3) $J_0(\chi_1,\dots,\chi_{r-1},\rho^{-1})=\rho(-1)(p-1)J(\chi_1,\dots,\chi_{r-1})$ *while* $J_0(\chi_1,\dots,\chi_r)=0$ *if* $\lambda\neq\varepsilon$.
(4) $J(\chi_1,\dots,\chi_r)=\frac{\prod_{i=1}^rG(\chi_i)}{G(\lambda)}$ *if* $\lambda\neq\varepsilon$, *while* $J(\chi_1,\dots,\chi_{r-1},\rho^{-1})=-\rho(-1)\frac{\prod_{i=1}^{r-1}G(\chi_i)}{G(\rho)}$.

PROOF. The first two claims are clear. For the third claim,

$$J_0(\chi_1,\dots,\chi_r)=\sum_{a_i\in(\mathbb{Z}/p\mathbb{Z})^{r-1}}\prod_{i=1}^{r-1}\chi_i(a_i)\chi_r(-\sum_i a_i)=\chi_r(-1)\sum_{t\neq0}\left[\sum_{\sum_{i=1}^{r-1}a_i=t}\chi_i\left(\frac{a_i}{t}\right)\right]\lambda(t)=\chi_r(-1)J(\chi_1,\dots,\chi_{r-1})\sum_{t\neq}$$

If $\chi_r=\rho^{-1}$ and $\lambda=\varepsilon$ then $\sum_{t\neq0}\lambda(t)=\sum_{t\neq0}1=p-1$. Otherwise, $\sum_{t\neq0}\lambda(t)=0$.

For the second part of the fourth claim, note that

$$\begin{aligned}\prod_{i=1}^{r} G(\chi_i) &= \sum_{a_i}\prod_{i}\chi_i(a_i)\zeta^{\sum_i a_i} \\ &= J_0(\chi_1,\ldots,,\chi_r)+\left[\sum_{t\neq 0}\lambda(t)\zeta_p^t\right]J(\chi_1,\ldots,\chi_r)\,.\end{aligned}$$

If $\lambda\neq\varepsilon$ then the J_0 term vanishes, the sum over t is $G(\lambda)$ and we have the second part of the claim. If $\lambda=\varepsilon$ the sum over t is (-1), $J_0(\chi_1,\ldots,\chi_r)=\chi_r(-1)(p-1)J(\chi_1,\ldots,\chi_{r-1})$ and $\prod_{i=1}^{r-1}G(\chi_i)=G(\rho)J(\chi_1,\ldots,\chi_{r-1})$. We conclude that

$$J(\chi_1,\ldots,\chi_r)=\left\{\rho(-1)(p-1)-G(\rho^{-1})G(\rho)\right\}J(\chi_1,\ldots,\chi_{r-1})\,.$$

Since $G(\rho)G(\rho^{-1})=p\rho(-1)$ we are done. □

COROLLARY 71. *Let $\chi_i\neq\varepsilon$. Then $|J(\chi_1,\ldots,\chi_r)|=p^{\frac{r-1}{2}}$ if $\prod_i\chi_i\neq\varepsilon$, $|J(\chi_1,\ldots,\chi_r)|=p^{\frac{r}{2}-1}$ otherwise.*

Math 437/537: Problem set 5 (due 13/11/09)

Quadratic reciprocity

1. Let p be a prime such that $q = 2p+1$ is also prime. Assuming $p \equiv 3\,(4)$ show that $q|2^p - 1$. Conclude that, with one exception, $2^p - 1$ is not prime.
   Hint: Consider $\left(\frac{2}{q}\right)$.

2. Let χ be the quadratic character mod p. Show that $G(\chi) = \sum_{t=0}^{p-1} \zeta_p^{t^2}$.

Jacobi sums

Let $l_1, \ldots, l_r \geq 1$, let $a_1, \ldots, a_r, b \in \mathbb{Z}$ be non-zero. We will study the equation

$$\sum_{i=1}^{r} a_i x_i^{l_i} = b\,.$$

3. Let N denote the number of solutions of the equation as a congruence mod p (a prime).
   (a) Assuming p does not divide b nor any of the a_i, express N in the form
   $$N = \sum_{\chi_1,\ldots,\chi_r} C(\chi_1,\ldots,\chi_r)\cdot J(\chi_1,\ldots,\chi_r)$$
   where the summation ranges over certain r-tuples of characters and the coefficients C have modulus 1.
   (b) Under these assumptions, find integers M_0, M_1 so that
   $$\left|N - p^{r-1}\right| \leq M_0 p^{(r/2)-1} + M_1 p^{(r-1)/2}\,.$$
   (c) Find an upper bound on M_0, M_1 depending only on $\underline{l}$ and conclude that if p is large enough (with an explicit lower bound depending only on $\underline{l}$, $\underline{a}$, b), the congruence has a non-zero solution.
   (d) Show that, if p is large enough, the existence of a solution mod p guarantees a solution mod p^k for all k.

4. Find a simple criterion for the existence of a real solution to the equation.

REMARK. With appropriate assumptions on the l_i and on r, the equation $\sum_{i=1}^{r} a_i x^{l_i} = b$ will have solutions in $\mathbb{Q}$ ("global solutions") iff it has solutions in $\mathbb{R}$ and in $\mathbb{Z}/p^k\mathbb{Z}$ for each p, k ("local solutions"). We have shown that checking whether there are local solutions is a finite process.

Arithmetical Functions

- $I(n) = \left[\frac{1}{n}\right]$, $\varepsilon(n) = 1$, $N(n) = n$.
- $\omega(n) = \#\{p \text{ prime} : p|n\}$ i.e. $\omega(\prod_p p^{e_p}) = \sum_p \min\{e_p, 1\}$ and $\Omega(\prod_p p^{e_p}) = \sum_p e_p$.
- Möbius function $\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \,\square\text{free} \\ 0 & \text{otherwise} \end{cases}$, Liouville function $\lambda(n) = (-1)^{\Omega(n)}$.
- von Mangoldt function $\Lambda(n) = \begin{cases} \log p & n = p^k, k \geq 1 \\ 0 & \text{otherwise} \end{cases}$.
- The divisor function $\tau = d = \sigma_0 = \varepsilon * \varepsilon = \#\{a : a|n\}$ and its generalizations $\sigma = \sigma_1 = \varepsilon * N$ and $\sigma_k = \varepsilon * N^k = \sum_{d|n} d^k$.

DEFINITION. The *Dirichlet convolution* of two arithmetical functions $f, g\colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$ is the arithmetical function

$$(f * g)(n) = \sum_{ab=n} f(a)g(b),$$

where the sum is over all pairs $(a,b) \in \mathbb{Z}^2_{\geq 1}$ such that $ab = n$.

5. Show that $*$ is associative and commutative, and that it is distributive over pointwise addition of functions. Show that I is an identity for the operation.

6. (Multiplicative functions) Let f, g be multiplicative functions.
   (a) Show that $f * g$ is multiplicative as well.
   (b) Say $f(p^k) = g(p^k)$ for all primes p and $k \geq 0$. Show that $f = g$.
   (c) Assuming f is not identically zero, show that $f(1) = 1$.

7. (Möbius inversion)
   (a) Let f be a non-zero multiplicative function. Show that there exists a multiplicative function f^{-1} so that $f * f^{-1} = I$.
   Hint: Define f^{-1} on prime powers first.
   (b) Conclude that if $f, f * g$ are multiplicative and f is non-zero then so is g.
   (c) Show that $\mu * \varepsilon = I$. Obtain the *Möbius inversion formula*: for any two arithmetical functions F, f we have $F(n) = \sum_{d|n} f(d)$ iff $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$.
   (d) Show that $\Lambda * \varepsilon = \log$ and hence that $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.
   Hint: consider $\sum_{d|n} \mu(d) \log \frac{n}{d}$ as well.

8. (The divisor function)
   (a) For each integer $n \geq 1$ show that there exists an integer $k \geq 1$ so that $\tau(nk) = n$.
   (b) Starting with $n_0 \geq 1$ set $n_{i+1} = \tau(n_i)$. Show that if n_0 is composite then some n_i is a perfect square.

9. (Some bounds) In the MathSciNet seminar we discussed the problem of integral values of the function $\frac{\phi(n)+\sigma(n)}{n}$.
   (a) Let $p < q$ be primes and let $n = p^\alpha q^\beta$. Show that $\frac{\varphi(n)+\sigma(n)}{n} = 2 + O(\frac{1}{p^2})$, and conclude that if $\frac{\phi(n)+\sigma(n)}{n}$ is an integer then it is equal to 2.
   (b) Show that there exists a function $f(k)$ so that $\frac{\sigma(n)}{n} \leq f(\omega(n))$ for all n.

CHAPTER 5

Quadratic forms

5.1. Definitions

DEFINITION 72. An *form* is a homogenous polynomial. We call a form *quadratic* if it is of degree 2, *cubic* if of degree 3 etc. We call a form *binary* if it has two variables, *ternary* if three and so on.

EXAMPLE 73. x^2+y^2 is a binary quadratic form, $\sum_{i=1}^{d} a_i x_i^2$ is a quadratic form, while x^3+y^3+zwv is a cubic form. The general *binary quadratic form* is then $f(x,y)=ax^2+bxy+cy^2$, in which case we can write

$$f(x,y)=\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

The matrix doesn't have to be integral!

DEFINITION 74. The *discriminant* of $ax^2+bxy+cy^2$ is $d=b^2-4ac$.

LEMMA 75. *f is a quadratic form iff $f(a\underline{x})=a^2 f(\underline{x})$ and $B(\underline{u},\underline{v})=f(\underline{u}+\underline{v})-f(\underline{u})-f(\underline{v})$ is a symmetric bilinear form.*

EXAMPLE 76. In general, a symmetric bilinear form (that is, a symmetric matrix A) gives rise to the quadratic form $f(\underline{x})=\underline{x}^T A\underline{x}$. Conversely, if 2 is invertible a quadratic form f comes from the bilinear form $\frac{1}{2}(f(\underline{u}+\underline{v})-f(\underline{u})-f(\underline{v}))$.

LEMMA 77. *Let f be a quadratic form with complex coefficients. Then $f(\mathbb{Z}^d)\subset\mathbb{Z}$ iff f has integral coefficients.*

PROOF. Sufficiency is clear. Conversely, say $f(\underline{x})=\sum_{i\le j} a_{ij}x_i x_j$. Then $a_{ii}=f(\underline{e}_i)$ while for $i<j$ we have $a_{ij}=f(\underline{e}_i+\underline{e}_j)-f(\underline{e}_i)+f(\underline{e}_j)$. □

COROLLARY 78. *An integral quadratic form is given by a symmetric matrix with entries in $\frac{1}{2}\mathbb{Z}$, except that diagonal entries must be integral.*

DEFINITION 79. Call the quadratic form f *degenerate* if there exists $\underline{u}\neq 0$ so that $f(\underline{u})=0$ and $B(\underline{u},\underline{v})=0$ for all $\underline{v}$ (that is, $f(\underline{v}+\underline{u})=f(\underline{v})$ for all $\underline{v}$). A non-degenerate form is *isotropic* if there exists $\underline{u}\neq 0$ so that $f(\underline{u})=0$, *anisotropic* otherwise.

LEMMA 80. *A non-degerate real quadaratic form is* isotropic *iff it takes both positive and negative values. Call the two cases* definite *and* indefinite.

PROOF. If $f(\underline{u})>0$ and $f(\underline{v})<0$ then f has a zero in $[\underline{u},\underline{v}]\not\ni\underline{0}$ since f is non-negative at all multiples of $\underline{u}$. Since $\nabla f(\underline{u})=\underline{u}^T B$, if f is non-degenerate and isotropic it takes both negative and positive values. □

- Why q. forms? *structure*.

Note: $d \equiv 0,1\,(4)$, and conversely we have the *principal forms* $x^2-(d/4)y^2$ or $x^2+xy-(\frac{d-1}{4})y^2$ with discriminant d. If $b^2-d=4nc$ then $nx^2+bxy+cy^2$ properly represents n. If $ax^2+bxy+cy^2=n$ with $(x,y)=1$ then

$$4a^2x^2+4abxy+4acy^2=4an$$

so

$$(2ax+by)^2+\left(4ac-b^2\right)y^2=4an$$

and similarly

$$(2cy+bx)^2-dx^2=4cn$$

For each $p^r\|4n$, either x or y is invertible mod p^r. It follows that d is a square mod $4n$.

5.2. Space of lattices & Reduction

Let f be a quadratic form on $\mathbb{R}^d$. We can change co-ordinates: given $\gamma \in \mathrm{GL}_d(\mathbb{R})$, $f\circ\gamma$ is another quadratic form taking the same values. In terms of the bilinear form we are moving from B to $\gamma^T B\gamma$. This is an action of $\mathrm{GL}_d(\mathbb{R})$ on the space of quadratic forms.

Similarly for f a quadratic form on $\mathbb{Z}^d$ and $\gamma \in \mathrm{GL}_d(\mathbb{Z})$.

THEOREM 81. *(Sylvester's "Law of intertial") Orbit representatives for this action are the diagonal forms with* $0,\pm1$ *on the diagonal.*

COROLLARY 82. *A real-valued quadratic form on* $\mathbb{Z}^d$ *up to choice of basis for* $\mathbb{Z}^d$ *is equivalent to a lattice* $\Lambda\subset\left(\mathbb{R}^d,g\right)$ *where* g *is one of these forms, up to isometry of* $\mathbb{R}^d$.

DEFINITION 83. Call $ax^2+bxy+cy^2$ *reduced* if $0\le b\le|a|=|c|$ or $-|a|<b\le|a|<|c|$.

PROPOSITION 84. *Every form is equivalent to a reduced one.*

PROOF. Act by $S=\begin{pmatrix}&-1\\1&\end{pmatrix}$ and $T=\begin{pmatrix}1&1\\&1\end{pmatrix}$ to get a form such that $|a|\le|c|$ and $-|a|<b\le|a|$. If $|a|=|c|$ then acting by S reverses the sign of b so may assume $b\ge0$.

Equivalent understanding: to a real definite form attach the root $\tau\in\mathbb{H}$ of az^2+bz+c. Then root of $f\circ\gamma$ is $\gamma\tau=\frac{\alpha\tau+\beta}{c\tau+\delta}$, and $y(\gamma\tau)=\frac{y(\tau)}{|c\tau+d|^2}$. □

COROLLARY 85. $\langle S,T\rangle=\mathrm{SL}_2(\mathbb{Z})$.

PROOF. $\tau=2i$ is reduced, has trivial stabilizer. □

LEMMA 86. $\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}\begin{pmatrix}a&b/2\\b/2&c\end{pmatrix}\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}=$

Suppose $(x,y)=1$. $y=0$ *makes* $x=\pm1$, $q(\pm1,0)=a$. $y=\pm1$ *and* $|x|\ge2$ *gives* $|2ax+by|\ge4a-a\ge3a$ *and so* $4af(x,y)=(2ax+by)^2-dy^2\ge9a^2-d>a^2-b^2+4ac\ge4ac$ *and* $f(x,y)>c$. $|y|\ge2$ *gives* $(2ax+by)^2-dy^2\ge-4d=16ac-4b^2=12ac+4(ac-b^2)>4ac$ *so again* $f(x,y)>c$. $q(0,\pm1)=c$. $q(\pm1,\pm1)=a+b+c>c$, *and* $q(\pm1,\mp1)=a-b+c>c$ *unless* $a=b$, *and* $>a$ *unless* $a=b=c$.

DEFINITION 87. $H(d)$ is class number at (non-square) discriminant d. $h(d)$ class number of reduced forms.

THEOREM 88. *(Heegner, Stark-Baker) For* $d<0$ $h(d)=1$ *iff* $d\in\{-3,-4,-7,-8,-11,-19,-43,-67,-163$

PROPOSITION 89. $H(d) \ll d$.

CHAPTER 6

Diophantine Approximation and Continued Fractions

6.1. Diophantine approximation

Given a real number ξ would like to find $r = \frac{a}{b} \in \mathbb{Q}$ so that $\left|\xi - \frac{a}{b}\right|$ is "small".

LEMMA 90. *Given ξ and $b \geq 1$ there is a so that $\left|\xi - \frac{a}{b}\right| \leq \frac{1}{2b}$.*

PROOF. Let a be the nearest integer to $b\xi$. Then $|b\xi - a| \leq \frac{1}{2}$. □

NOTATION 91. $\{y\} = y - \lfloor y \rfloor$, $\|y\| = d(y,\mathbb{Z}) = \min\{\{y\}, 1-\{y\}\}$.

When ξ is rational can't do very well:

LEMMA 92. *(Discreteness principle) Let $\frac{p}{q}, \frac{a}{b} \in \mathbb{Q}$. If $\frac{p}{q} \neq \frac{a}{b}$ then $\left|\frac{p}{q} - \frac{a}{b}\right| = \left|\frac{pb-aq}{qb}\right| \geq \frac{1}{qb}$.*

PROPOSITION 93. *(Pigeon-hole principle) Given ξ, n there are $a, b \in \mathbb{Z}$ with $1 \leq b \leq n$ so that $\left|\xi - \frac{a}{b}\right| \leq \frac{1}{b(n+1)} < \frac{1}{b^2}$.*

PROOF. $\{\{k\xi\}\}_{k=0}^{n+1} \subset [0,1)$ is a set of size $n+2$. It follows that two of its members differ by at most $\frac{1}{n+1}$. Say that $0 \leq \{k\xi\} - \{l\xi\} \leq \frac{1}{n+1}$ for some $0 \leq k \neq l \leq n+1$. Then $\{(k-l)\xi\} = \{k\xi\} - \{l\xi\} \leq \frac{1}{n+1}$, so $\||k-l|\xi\| \leq \frac{1}{n+1}$. With $b = |k-l|$ we have found a so that $\left|\xi - \frac{a}{b}\right| \leq \frac{1}{b(n+1)}$. □

COROLLARY 94. *For $\xi \in \mathbb{R} \setminus \mathbb{Q}$ there are infinitely many b for which there exists a such that $\left|\xi - \frac{a}{b}\right| < \frac{1}{b^2}$.*

PROOF. For each n choose a_n, b_n so that $\left|\xi - \frac{a_n}{b_n}\right| \leq \frac{1}{b_n(n+1)} < \frac{1}{b_n^2}$. The b_n cannot be bounded since $d(\xi, \frac{1}{M!}\mathbb{Z}) > 0$. □

The bound in the proposition si optimal up to constants:

THEOREM 95. *(Liouville) let $\alpha \in \mathbb{R}$ be an algebraic number of degree d. Then $\left|\alpha - \frac{a}{b}\right| \gg_\alpha \frac{1}{b^d}$ for all $a, b \in \mathbb{Z}$ with $b \geq 1$.*

PROOF. Let $f \in \mathbb{Z}[x]^{\leq d}$ be such that $f(\alpha) = 0$ and consider $\frac{f(\alpha) - \frac{a}{b}}{\alpha - \frac{a}{b}}$. □

Math 437/537: Problem set 6 (due 4/12/09)

Prime estimates

1. In class we found $0 < \delta < 1 < \Delta$ so that $\delta x \leq \nu(x) \leq \Delta x$ for $x \geq 2$. Complete the proof of Chebychev's Theorem by finding $0 < A < B$ so that $A\frac{x}{\log x} \leq \pi(x) \leq B\frac{x}{\log x}$ if $x \geq 2$.

2. Find $0 < C < D$ so that $C \log\log x \leq \sum_{p \leq x} \frac{1}{p} \leq D \log\log x$ for $x \geq 3$.
   Hint: Break the range of summation into dyadic intervals $\left[2^j \leq p < 2^{j+1}\right]$.

OPT (The average number of prime divisors) Let $P(x) = \frac{1}{x}\sum_{n \leq x} \omega(n)$.

(a) Show that $P(x) = \frac{1}{x}\sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor$ (sum over primes).
   Hint: Write $\omega(n) = \sum_{p|n} 1$ and change the order of summation.

(b) Show that $C \log\log x - 1 \leq P(x) \leq D \log\log x$ for $x \geq 3$.
   Hint: $y - 1 \leq \lfloor y \rfloor \leq y$.

(c) Mertens has found E so that $\left|\sum_{p \leq x} \frac{1}{p} - \log\log x\right| \leq E$ for all x. Conclude that $|P(x) - \log\log x|$ is uniformly bounded as well.

— This result is usually phrased: "the average number of distinct primes dividing a random integer is about $\log\log x$".

Irrationality and continued fracionts

3. Show that the following numbers are irrational:
   (a) $\frac{\log n}{\log m}$ where $n, m \geq 2$ are relatively prime integers.
   (b) $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.
   Hint: Consider $\lfloor k!e \rfloor$.
   (c) $\sum_{n=0}^{\infty} \frac{1}{3^{4^n}}$.
   Hint: Multiply by a power of 3 and consider the fractional part.

OPT (Egyptian fractions) Show that $r \in \mathbb{Q} \cap (0,1)$ can be written in the form $r = \sum_{i=1}^{t} \frac{1}{q_i}$ with distinct $q_i \in \mathbb{Z}_{>0}$.

4. (Hermite) Let p be a prime such that $p \equiv 1\,(4)$. Let $0 < u < p$ with $u^2 \equiv -1\,(p)$. Write $\frac{u}{p} = \langle a_0, \ldots, a_n \rangle$ and let i be maximal such that $k_i \leq \sqrt{p}$.
   (a) Show that $\left|\frac{h_i}{k_i} - \frac{u}{p}\right| < \frac{1}{k_i\sqrt{p}}$. Conclude that $|h_i p - u k_i| < \sqrt{p}$.
   (b) Let $x = k_i$, $y = h_i p - u k_i$. Show that $0 < x^2 + y^2 < 2p$. Show that $x^2 + y^2 \equiv 0\,(p)$ and conclude that $p = x^2 + y^2$.
5. Calculate the 0th through 4th convergents to π.

6. (Convergence)
   (a) Suppose the infinite continued fractio n exapnsions of θ, η agree through a_n. Show that

   $$|\theta - \eta| \leq \frac{1}{k_n^2}.$$

(b) Show that $\lim_{n\to\infty}\langle a_0,a_1,\ldots,a_n,b_{n+1},b_{n+2},\ldots\rangle = \langle a_0,a_1,\ldots\rangle$.

The continued fraction expansion of e.

Set $(-1)!! = 0!! = 1$ and for $n \geq 1$,

$$n!! = \prod_{\substack{1\leq j\leq n\\ j\equiv n\,(2)}} j\,.$$

Now for $n \geq 0$ set:

$$\psi_n(x) = \sum_{k=0}^{\infty} \frac{x^{2k}}{(2k+2n-1)!!(2k)!!} \qquad , w_n(n) = \frac{\psi_n(x)}{x\psi_{n+1}(x)}\,.$$

7. (Evaluation)
   (a) Show that $\psi_n(x)$ are entire functions.
   (b) Show that $\psi_0(x) = \cosh(x) = \frac{e^x+e^{-x}}{2}$ and that $\psi_1(x) = \frac{\sinh(x)}{x} = \frac{e^x-e^{-x}}{2x}$. Conclude that $w_0(x) = \tanh(x) = \frac{e^x+e^{-x}}{e^x-e^{-x}}$.
   (d) Show that $\psi_n(x) = (2n+1)\psi_{n+1} + x^2\psi_{n+2}$. Conclude that $w_n(x) = \frac{2n+1}{x} + \frac{1}{w_{n+1}(x)}$.
   (e) Using your answer to part (d) show that $\frac{e^{1/k}+e^{-1/k}}{e^{1/k}-e^{-1/k}} = \langle k,3k,5k,7k,9k,\cdots\rangle$ for all $k \geq 1$.

8. (Calculation)
   (a) Let $u = w_0(\frac{1}{2})$ and let $v = \langle v_0,v_1,v_2,v_3,\ldots\rangle$ where $v_0 = 0$, $v_1 = 5 = 2\cdot(2\cdot 1+1)-1$ and $v_n = 2(2n+1)$ for $n \geq 2$. Show that $u = 2 + \frac{1}{1+\frac{1}{v}}$
   (b) Show that $e = \frac{u+1}{u-1} = \langle 2,1+2v\rangle$.
   (c) Let ξ be a real number, $b \geq 2$ an integer, and let $\alpha = \langle 0,2b\text{–}1,\xi\rangle$. Show that $2\alpha = \left\langle 0;b-1,1,1+\frac{2}{\xi-1}\right\rangle$.
   (d) Let $\{b_n\}_{n=1}^{\infty} \subset \mathbb{Z}_{\geq 2}$ and let $\alpha = \langle 0,2b_1-1,2b_2,2b_3,\ldots\rangle$. Show that
   $$2\alpha = \langle 0,b_1-1,1,1,b_2-1,1,1,b_3-1,1,1,\ldots\rangle\,.$$

9. (Punchline) Show that
   $$e = \langle 2,1,2,1,1,4,1,1,6,1,1,8,1,1,10,\cdots\rangle = \langle 2,1,e_2,e_3,e_4,\cdots\rangle$$
   where $e_n = \begin{cases} 2k & n = 3k-1 \\ 1 & n \equiv 0,1\,(3)\end{cases}$.

6.2. Continued fractions

Note that $\mathrm{PGL}_2(\mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$.

DEFINITION 96. For a sequence of complex numbers $\{a_i\}_{i=0}^{\infty}$ we define a seqeunce of functions as follows:

$$F_{-1}(z) = \langle z \rangle \stackrel{\text{def}}{=} z$$

and for $n \geq 0$,

$$F_n(z) = \langle a_0, \ldots, a_n, z \rangle \stackrel{\text{def}}{=} \left\langle a_0, \ldots, a_n + \frac{1}{z} \right\rangle .$$

We also set

$$r_n \stackrel{\text{def}}{=} \langle a_0, \ldots, a_n \rangle = F_{n-1}(a_n) = F_n(\infty) .$$

PROPOSITION 97. *There exist $\{h_n\}_{n=-2}^{\infty}$, $\{k_n\}_{n=-2}^{\infty}$ so that $F_n(z) = \frac{h_n z + k_n}{h_{n-1} z + k_{n-1}}$. In fact, taking $h_{-1} = 1$, $h_{-2} = 0$, $k_{-1} = 0$, $k_{-2} = 1$, and $h_n = h_{n-1}a_n + h_{n-2}$ and $k_n = k_{n-1}a_n + k_{n-2}$ works.*

PROOF. Let $g_n = \begin{pmatrix} a_n & 1 \\ 1 & \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$, let $f_n = g_0 \cdots g_n$. Writing $G_n(z) = g_n \cdot z$ we have $F_{-1} = I \cdot z$ and $F_n = F_{n-1} \circ G_n$ so $F_n(z) = g_n \cdot z$. Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} ae+b & a \\ ce+d & c \end{pmatrix}$ the claim follows. □

COROLLARY 98. $\det(f_n) = (-1)^{n-1}$. *In particular,*

$$\begin{aligned} r_n - r_{n-1} &= \frac{\det(f_n)}{k_n k_{n-1}} \\ &= \frac{(-1)^{n-1}}{k_n k_{n-1}} . \end{aligned}$$

It also follows that

$$\begin{aligned} r_n - r_{n-2} &= (-1)^{n-1} \left[\frac{1}{k_n k_{n-1}} - \frac{1}{k_{n-1} k_{n-2}} \right] \\ &= \frac{(-1)^{n-1}}{k_n k_{n-2}} \frac{k_{n-2} - k_n}{k_{n-1}} \\ &= \frac{(-1)^n}{k_n k_{n-2}} a_n \end{aligned}$$

Assume now that $\{a_n\}_{n=0}^{\infty}$ are positive integers. Then $f_{-1}, g_n \in \mathrm{GL}_2(\mathbb{Z})$ for all n so $f_n \in \mathrm{GL}_2(\mathbb{Z})$ for all n. This already shows that $(h_n, k_n) = 1$ for all n. Moreover, h_{n-2} is bounded below by the nth Fibbonachi number ($h_n \geq h_{n-1} + h_{n-2}$) and k_n grows similarly (same inequality just different initial conditions). It follows that $r_n - r_{n-1}$ decreases exponentially so the sequence $\{r_n\}_{n=0}^{\infty}$ converges.

REMARK 99. We will allow a_0 to be any integer, noting that $\langle a_0, \ldots, a_n \rangle = a_0 - 1 + \langle 1, a_1, \ldots, a_n \rangle$ if $n \geq 0$. The same convergence proof applies.

DEFINITION 100. An *infinite simple continued fraction* is an expression $\langle a_0, a_1, \ldots \rangle$ with a_n integers, positive except possible for a_0. Its value is by definition $\lim_{n\to\infty} r_n$.

THEOREM 101. *The value $\theta = \langle a_0, \ldots \rangle$ is irrational.*

PROOF. We use $r_n - r_{n-2} = \frac{(-1)^n}{k_n k_{n-2}} a_n$, which implies $r_0 < r_2 < r_4 < \ldots$ and $r_1 > r_3 > \cdots$. This shows that $r_n \neq \theta$ for all n, in fact that

$$0 < |\theta - r_n| < |r_{n+1} - r_n| .$$

Multiplying by k_n we find:

$$0 < |k_n\theta - h_n| < \frac{1}{k_{n+1}} .$$

If θ was rational, $|k_n\theta - h_n|$ would be uniformly bounded away from zero, a contradiction. □

PROPOSITION 102. *Let $\theta = \langle a_0, \ldots \rangle$. Then $a_0 = \lfloor \theta \rfloor$ and $\theta = a_0 + \frac{1}{\theta_1}$ where $\theta_1 = \langle a_1, \ldots \rangle$.*

PROOF. Note that $r_0 < \theta < r_1$, that is $a_0 < \theta < a_0 + \frac{1}{a_0}$. Since $a_1 \geq 1$ we get the first claim. For the second, note that $f_n = g_0(g_1 \cdots g_n)$, that is $\langle a_0, a_1, \cdots, a_n, z \rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n, z \rangle}$. Setting $z = \infty$ and taking $n \to \infty$ gives the claim. □

COROLLARY 103. *If $\langle a_0, \ldots \rangle = \langle b_0, \ldots \rangle$ then $a_n = b_n$ for all n.*

PROOF. The Lemma gives $a_0 = b_0$ and $\langle a_1, \ldots \rangle = \langle b_1, \ldots \rangle$. □

THEOREM 104. *Given $\xi \in \mathbb{R}$ set $\xi_0 = \xi$, and for $n \geq 0$ set $a_n = \lfloor \xi_n \rfloor$, $\xi_{n+1} = \frac{1}{\xi_n - a_n}$. Then $\xi_n > a_n \geq 1$ for all $n \geq 1$ and*

$$\xi = \langle a_0, a_1, \ldots \rangle .$$

If ξ is rational the process terminates after finitely many steps and we have equality.

PROOF. By induction we have $\xi = \langle a_0, \ldots, a_n, \xi_{n+1} \rangle = F_n(\xi_{n+1})$ and $r_{n+1} = F_n(a_{n+1})$. It follows that

$$\begin{aligned} \xi - r_n &= F_n(\xi_{n+1}) - \frac{h_n}{k_n} \\ &= \frac{h_n\xi_{n+1} + h_{n-1}}{k_n\xi_{n+1} + k_{n-1}} - \frac{h_n}{k_n} \\ &= \frac{(-1)^n}{k_n(k_n\xi_{n+1} + k_{n-1})} , \end{aligned}$$

so

$$|\xi - r_n| \leq \frac{1}{k_n k_{n+1}} \xrightarrow[n\to\infty]{} 0$$

since $\xi_{n+1} \geq a_{n+1}$. □

COROLLARY 105. $|k_n\xi - h_n| = \frac{1}{k_n\xi_{n+1} + k_{n-1}} < \frac{1}{k_n}$. *In particular, $|k_n\xi - h_n|$ and $|\xi - r_n|$ are decreasing.*

PROOF. The first claim is immediate. for the second note that $k_{n-1}\xi_n + k_{n-2} < k_{n-1}(a_n + 1) + k_{n-2} = k_n + k_{n-1} < k_n\xi_{n+1} + k_{n-1}$. □

Note that

$$\begin{aligned} F_n(x)-F_n(y) &= \frac{h_nx+h_{n-1}}{k_nx+k_{n-1}}-\frac{h_ny+h_{n-1}}{k_ny+k_{n-1}} \\ &= \frac{(h_nk_{n-1}-h_{n-1}k_n)(x-y)}{(k_nx+k_{n-1})(k_ny+k_{n-1})} \end{aligned}$$

THEOREM 106. *Let $a,b\in\mathbb{Z}$ with $b>0$. If $\left|\theta-\frac{a}{b}\right|<|\theta-r_n|$ then $b>k_n$. If $|b\theta-a|<|k_n\theta-h_n|$ then $b\geq k_{n+1}$.*

PROOF. Let $a,b\in\mathbb{Z}$ with $0<b<k_{n+1}$ (so $\frac{a}{b}\neq r_{n+1}$) and $\frac{a}{b}\neq r_n$. We have $F_{n+1}(0)=r_n$, $F_{n+1}(\infty)=r_{n+1}$ and

$$\begin{aligned} F'_{n+1}(z) &= \frac{h_{n+1}(k_{n+1}z+k_n)-k_{n+1}(h_{n+1}z+h_n)}{(k_{n+1}z+k_n)^2} \\ &= \frac{\det(f_{n+1})}{(k_{n+1}z+k_n)^2}\,. \end{aligned}$$

It follows that $(-1)^nF'_{n+1}(0)>0$. Since F_{n+1} is bijective on $\mathbb{P}^1(\mathbb{R})$ it follows that $F_{n+1}([0,\infty])=[r_n,r_{n+1}]$. Now let $\frac{x}{y}\in\mathbb{P}^1(\mathbb{Q})$ satisfy $F_{n+1}(\frac{x}{y})=\frac{a}{b}$. Then $\frac{x}{y}\neq 0,\infty$ and we have $k_{n+1}x+k_ny=b$. Since $0<b<k_{n+1}$ this forces x,y to have opposite signs, so $\frac{x}{y}\notin[0,\infty]$ and hence $\frac{a}{b}\notin[r_n,r_{n+1}]$, so $\left|\theta-\frac{a}{b}\right|<|\theta-r_{n+1}|$. This establishes the first claim. For the second note that

$$\begin{aligned} |b\theta-a| &= |k_{n+1}x\theta+k_ny\theta-h_{n+1}x-h_{n+1}\theta| \\ &= |x(k_{n+1}\theta-h_{n+1})+y(k_n\theta-h_n)| \\ &= |x|\,|k_{n+1}\theta-h_{n+1}|+|y|\,|k_n\theta-h_n| \end{aligned}$$

since $\theta-r_{n+1}$, $\theta-r_n$ also have opposite signs. Since $|x|,|y|\geq 1$ we find the claim. □

LEMMA 107. *Let $\xi\in\mathbb{R}$ be irrational and $\frac{a}{b}\in\mathbb{Q}$ satisfy $\left|\xi-\frac{a}{b}\right|<\frac{1}{2b^2}$. Then $\frac{a}{b}$ is a convergent of ξ.*

PROOF. There is n so that $k_n\leq b<k_{n+1}$. We will show that $b=k_n$. Otherwise we have $\frac{1}{k_nb}\leq\left|\frac{a}{b}-\frac{h_n}{k_n}\right|\leq\left|\xi-\frac{a}{b}\right|+\left|\xi-\frac{h_n}{k_n}\right|<\frac{1}{2b^2}+\frac{1}{k_n}|k_n\xi-h_n|<\frac{1}{2b^2}+\frac{1}{k_n}\frac{b}{2b^2}$ since $|k_n\xi-h_h|<|b\xi-a|$. This gives $b<k_n$, a contradiction. □

LEMMA 108. *Let $\xi\in\mathbb{R}_{>0}$ be irrational, let $A,B\in\mathbb{Z}_{>0}$ and let $A^2-B^2\xi^2=\sigma$ satisfy $0<\sigma<\xi$. Then $\frac{A}{B}$ is a convergent of ξ.*

PROOF. We have $\left|\xi-\frac{A}{B}\right|=\frac{1}{B}\frac{\left|B^2\xi^2-A^2\right|}{|B\xi+A|}=\frac{1}{B^2}\frac{\sigma}{\left|\xi+\frac{A}{B}\right|}<\frac{1}{B^2}\frac{\xi}{2\xi}$ since $\frac{A}{B}>\xi$. □

THEOREM 109. *Let $d\in\mathbb{Z}_{\geq 1}$ be squarefree. Then any positive solution to* Pell's equation *$x^2-dy^2=\pm 1$ is a convergent of $\sqrt{d}$.*

PROOF. For the positive sign this is the previous lemma. If $x^2-dy^2=-1$ then $y^2-\frac{1}{d}x^2=\frac{1}{d}$ and $0<\frac{1}{d}<\frac{1}{\sqrt{d}}$. It follows that $\frac{y}{x}$ is a convergent of $\frac{1}{\sqrt{d}}$, so $\frac{x}{y}$ is a convergent of $\sqrt{d}$. □

REMARK 110. At least for $d\geq 17$ the same holds for the equations $x^2-dy^2=\pm 4$ which are important when $d\equiv 1\,(4)$.

THEOREM 111. *The solutions to* $x^2 - dy^2 = \pm 1$ *take the form* $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$ *for* $n \in \mathbb{Z}$.

PROOF. Map solutions to $\mathbb{R}^2$ via $(x,y) \mapsto \left(\log\left|x+\sqrt{d}y\right|, \log\left|x-\sqrt{d}y\right|\right)$. The image is a discrete subgroup of a one-dimensional subspace. □

Bibliography

[1] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991.