Math 312: Introduction to Number Theory
Lecture Notes

Lior Silberman

These are rough notes for the winter 2021 course. Problem sets were posted on the course website; solutions on an internal website.

Contents

Introduction

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

0.1. Cold open

- Theory of "numbers", mainly meaning whole numbers, that is the integers.

Cryptography.

- Do you use the internet?
- Can use number theory to establish identity ("The person who knows the factorization $N = pq$")
  - Key (1): There are arithmetic problems that only the person who knows the factorization can solve.
  - Key (2): I can prove to you that I know to factor N without revealing this number.
- How do you know that https://www.yourbank.ca is really controlled by your bank? Roughly speaking:
  - The manufacturer of your browser equips it with a list of 230 numbers and told to trust those people who know how to factor them. Those people are called "certificate authorities". For simplicity assume there was only one CA, with its number N_{CA} built into the browser.
  - Your bank creates a number N_{bank} for itself. It goes to the CA and gets a "digital certificate", which says: "the people who know how to factor N_{CA} say that the server at https://www.yourbank.ca knows how to factor the number N_{bank}". Moreover, the certificate includes a number calculated using the details in it and also $p_{\text{CA}}, q_{\text{CA}}$ – so it cannot be forged.
  - When you access https://www.yourbank.ca, the website provides your browser with the certificate. Your computer can *verify* the signature using the number N_{CA} that it knows. If this is ok it then challenges the machine on the other side to prove that it can really factor the number N_{bank} specified in the certificate.
  - If that works too the browser is happy.
  - (I'm Lying a little here) When you type your password on https://www.yourbank.ca, what your browser sends is not simply the characters you type (that would be bad if there were eavesdroppers). What it sends instead is the result of a calculation involving the number N_{bank}. The calculation is done in such a way that the bank can check that you typed the correct password using its secret knowledge (p_{bank}, q_{bank}) – whereas the eavesdropper (who only knows N_{bank}) can't learn what the password was.

There are practical problems with this scheme, but we won't discuss internet security. What we will discuss is the *number theory* that makes secure websites possible.

Summary for those reading the notes:

- Underlying fact of life: arithmetic is "easy" but solving equations is "hard".
- There is a method for me to convince others that I know p, q without revealing them. This allows me to prove my identity ("I'm the person who knows to factor N"). But prevents forgery
- The method extends to verifiable signatures ("This email was written by the person who knows how to factor N"). No-one can forge my signature, but they can check I'm the person who signed (signing requires knowing p, q but checking only requires knowing N).
- The method extends to secure communication: you can take a message m and send me $F(m,N)$. Knowing p, q solving $F(m,N) = C$ is actually easy. But it is believed impossible to solve the equation knowing only N.
- We will discuss how to do all these things (signature protocol, secure communications protocol).

Other examples

- Software "product activation" key verification.

0.2. Administrivia

Syllabus distributed. Other key points:

- Webwork will be posted in the proper place.
- Problem sets will be posted on the course website. Solutions will be posted on a secure system (email explanation will be sent).
  - Depending on time, the grader may only mark selected problems. Solutions will be complete.
- Absolutely essential to
  - Read ahead according to the posted schedule. Lectures after the first will assume that you had done your reading.
  - Do homework.
- Office hours on Wednesdays and Thursdays after class. Also by appointment.
- Course website is important. Contains notes, problem sets, announcements, reading assignments etc.

0.3. More on problems of number theory

Some arithmetic.

- It is now 10am. What hour will it be 5 hours from now?
- Today is Tuesday, May 15th. What day was it 4 days ago?
  - What day of the week did 15/5/2017 fall on? Hint: $365 = 52 \cdot 7 + 1$.
  - What about July 1st, 1867? [don't wait for answer]

Properties of individual numbers.

- Can we find integers a, b so that $\left(\frac{a}{b}\right)^2 = 2$?

- We want to at least find integers a, b so that $\frac{a}{b}$ is close to $\sqrt{2}$. How well can we do this without taking b too large?
- Consider the decimal expansion of π (or e, or your favourite number). Do all the digits $0, 1, \ldots, 9$ appear $\frac{1}{10}$th of the time? What about all sequences $00, 01, \ldots, 99$?
- We already saw that primes are useful. We need to make primes.
  - How many primes are there? Are they easy to find?
  - Specifically: how does one tell if a given number n is prime?

Main focus: finding integer solutions to equations.

- All integer solutions to $x^2 + y^2 = z^2$ known to the Greeks (lots!)
  - Only obvious integer solutions to $x^4 + y^4 = z^4$ (Fermat)
  - Only obvious solutions to $x^3 + y^3 = z^3$ (Euler)
  - ...
  - Only obvious solutions to $x^n + y^n = z^n$, $n \geq 3$ (Ribet, Wiles)
- Other equations to solve:
  - $xy = N$ ("factorization"). Very important – we will discuss this.
  - $y = x + d$, $z = x + 2d$, $w = x + 3d$ ("arithmetic progression")
    - Szemeredi: if $A \subset \{1, \ldots, N\}$ is large enough then for some $d \neq 0$, A it contains x, y, z, w solving the above equation.
    - Green, Green-Tao: can take A to be the set of primes, or even a "dense subset" of the primes.
  - $p_1 - p_2 = 2$ ("twin primes")
  - $p_1 + p_2 = 2N$ ("Goldbach Conjecture")
- *Counting* solutions to equations
  - $\#\{1 \leq p \leq x \mid p \text{ prime}\} \approx \frac{x}{\log x}$ (Hadamard, de la Vallée-Poussin 1896 following Riemann 1859)
  - $\left|\#\{1 \leq p \leq x \mid p \text{ prime}\} - \frac{x}{\log x}\right| \leq C\sqrt{x}(\log x)^{100}$ ("Riemann hypothesis")

Much more.

- Not for today.

0.4. Course plan (subject to revision)

- The integers
  - Definition: induction and the well-ordering principle;
  - Multiplication: divisibility and the GCD, primes and unique factorization.
- Congruences [major point of the course]
- Algebra: primitive roots
  - The multiplicative group
  - Primality testing
  - Discrete log cryptosystems
- Application: public-key cryptography, RSA
- Multiplicative functions
- Quadratic reciprocity

References. Any book with the title “Elementary Number Theory” or “Introduction to Number Theory” will cover the material. I will generally follow the textbook “Elementary Number Theory and its applications” by K. Rosen.

CHAPTER 1

The Integers

1.1. The axioms; the well-ordering principle; induction

We record here the usual properties of the integers.

DEFINITION 1. The *integers* are the sextuple $(\mathbb{Z}, +, \cdot, 0, 1, <)$ satisfying:

- $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ("addition") and $\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ("multiplication") are binary operations; $0, 1 \in \mathbb{Z}$ are elements ("zero", "one") and $<$ is a binary relation ("less than").
- Addition is commutative and associative; $a + 0 = a$ and for all $a \in \mathbb{Z}$ there is $(-a) \in \mathbb{Z}$ so that $a + (-a) = 0$.
- Multiplication is commutative and associative; $a \cdot 1 = a$.
- The relation $<$ is transitive, and for all $a, b \in \mathbb{Z}$ exactly one of $a < b$, $a = b$, $b > a$ holds.
- For $a, b > 0$ we have $a + b, a \cdot b > 0$.
- **Well-ordering property**: every non-empty subset $A \subset \mathbb{N} = \mathbb{Z}_{\geq 0}$ has a least element.

Note that we interchangeably write $\mathbb{N}$ or $\mathbb{Z}_{\geq 0}$ for the set of *natural numbers*, those being the non-negative integers (0 is a natural number for us). Some books also uses the notation $\mathbb{Z}^+$ for the set $\mathbb{Z}_{>0} = \mathbb{Z}_{\geq 1}$ of *positive* integers.

The most important property is the last one. We illustrate it with several calculations. We first justify the last equality:

LEMMA 2. *(Discreteness) There is no integer b satisfying $0 < b < 1$.*

PROOF. Let $A = \{n \in \mathbb{Z} \mid 0 < n < 1\} \subset \mathbb{Z}_{\geq 0}$. Assume by contradiction that A is non-empty and let a be its minimal element. Then $0 < a < 1$. Multiplying both sides by a we find that $0 < a^2 < a < 1$. But then a^2 is an integer satisfying $0 < a^2 < 1$ so $a^2 \in A$ and $a^2 < a$, a contradiction to a being the smallest member of A. □

COROLLARY 3. *For any integer n there is no integer a satisfying $n < a < n + 1$.*

PROOF. If a existed set $b = a - n$. Then $0 < b < 1$. □

THEOREM 4. *(Principles of induction)*

(1) *(Weak induction) Let $P \subset \mathbb{N}$. Assume that $0 \in P$ and that for any number n, $n \in P \Rightarrow n + 1 \in P$. Then $P = \mathbb{N}$.*
(2) *(Strong induction) Let $P \subset \mathbb{N}$. Assume that for any $n \in \mathbb{N}$, $\{a \in \mathbb{N} \mid a < n\} \subset P \Rightarrow n \in P$. Then $P = \mathbb{N}$.*

PROOF. (1) Assume by contradiction that $P \neq \mathbb{N}$. Then the set $A = \mathbb{N} \setminus P$ of counterexamples is non-empty. Let m be its minimal element. Then $m \neq 0$ ($0 \in P$) so $m \geq 1$ and $m - 1 \in \mathbb{N}$. Since m was minimal, $m - 1 \notin A$ so $m - 1 \in P$. But then $m = (m - 1) + 1 \in P$, a contradiction.

(2) Let Q be the set of $n \in \mathbb{N}$ such that $\{a \in \mathbb{N} \mid a < n\} \subset P$. Then $0 \in Q$ (the set of natural numbers smaller than zero is empty). Also, if $n \in \mathbb{N}$ then $\{a \in \mathbb{N} \mid a < n\} \subset P$ so $n \in P$. But then

$\{a \in \mathbb{N} \mid a < (n+1)\} = \{a \in \mathbb{N} \mid a < n\} \cup \{n\} \subset P$ so $n+1 \in Q$. By part (1) it follows that $Q = \mathbb{N}$. Now for any $n \in \mathbb{N}$ we have that $n+1 \in Q$ and so that $n \in P$. □

DEFINITION 5. Call an integer n even *if it is of the form $n = 2k$ for some $k \in \mathbb{Z}$. Call it* odd *otherwise.*

THEOREM 6. *(Division by 2) Among every two consecutive natural numbers at least one is even.*

PROOF USING WELL-ORDERING. Let A be the set of $n \geq 0$ such that $n, n+1$ are both odd, and let m be a minimal member of A. Then both $m, m+1$ are odd so $m > 0$ (zero is even!) and $m-1 \geq 0$. Since m is minimal, $m-1 \notin A$, one of $m-1, m$ is even. m is odd so $m-1 = 2k$ for some $k \in \mathbb{Z}$. But then $m+1 = (m-1)+2 = 2(k+1)$ is even, a contradiction. Since A cannot have a least member it is empty. □

PROOF USING WEAK INDUCTION. Let P be the set of $n \geq 0$ such that at least one of $n, n+1$ is even. $0 \in P$ since it is even. Assume that $n \in P$. If $n+1$ is even then one of $n+1, n+2$ is even so $n+1 \in P$. Otherwise n must be even, so $n+2$ is also even and again $n+1 \in P$. □

Example in how to use well-ordering:

THEOREM 7. *(Division with remainder) Let $n, a \in \mathbb{Z}$ with $a > 0$. Then there are* unique *$q, r \in \mathbb{Z}$ with $0 \leq r < a$ such that*

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

PROOF. Let $T = \{m \in \mathbb{N} \mid \exists k \in \mathbb{Z} : m = n - ka\}$. In other words, T is the set of all natural numbers which differ from n by a multiple of a. T is non-empty, since by taking k sufficiently negative we can make $n - ka$ as large as we want (e.g. take $k = -|n|$). By the well-ordering principle there is $r = \min T$. By definition of T, we have $0 \leq r$ and there is $q \in \mathbb{Z}$ such that $r = n - qa$. Assume that $r \geq a$. Then $r - a \geq 0$ and $r - a = n - (q+1)a$ so $r - a \in T$, a contradiction. It follows that $n = qa + r$ for some q, r as claimed.

Assume next that also $n = q'a + r'$. Then

$$q'a + r' = n = qa + r\,.$$

Assume first that $r' > r$. Then

$$r' - r = (q - q')a\,,$$

so by the Lemma, $a > r' \geq r' - r \geq a$, a contradiction. By symmetry we can't have $r > r'$ either, so $r = r'$. It follows that $(q - q')a = 0$ and since $a \neq 0$ this means $q = q'$. □

COROLLARY 8. *An integer n is odd iff it can be written in the form $n = 2k+1$ for some $k \in \mathbb{Z}$.*

1.2. Divisibility and the GCD

1.2.1. Divisibility.

DEFINITION 9. Let $a, b \in \mathbb{Z}$. We say *a divides b* (and that b is a *multiple* of a) if there is $c \in \mathbb{Z}$ such that $b = ac$. When this holds we write $a|b$. Otherwise we say *a does not divide b* and write $a \nmid b$.

REMARK 10. Another way to phrase $a|b$ is that the equation $ax = b$ has a solution in $\mathbb{Z}$.

NOTATION 11. If $a|b$ with $a \neq 0$ we write $\frac{b}{a}$ for the (unique) integer x such that $a \cdot x = b$. Note that if $a \nmid b$ we don't give $\frac{b}{a}$ any meaning.

EXAMPLE 12. $1|b$ for all b. $0|b$ iff $b = 0$. $15|120$. For any $a, b \in \mathbb{Z}$ we have $(a-b)|(a^2-b^2)$. In particular, $2^{2^n} - 1 \mid 2^{2^{n+1}} - 1$.

LEMMA 13. *Let $a \neq 0$ and let $a|b$. Then $|b| \geq |a|$.*

PROOF. If $b = ac$ we have $|b| = |a|\,|c|$. Also, $|c| \geq 1$ since $c \neq 0$ so $|a|\,|c| \geq |a|$. □

LEMMA 14 (Euclid). *If a divides b and c then a divides $b \pm c$.*

PROOF. We have $a\left(\frac{b}{a} \pm \frac{c}{a}\right) = \left(a \cdot \frac{b}{a}\right) \pm \left(a \cdot \frac{c}{a}\right) = b \pm c$ so the equations $a \cdot x = b \pm c$ have an integer solution. □

COROLLARY 15. *Let $n \geq 1$. Then the only positive common divisor of $n, n+1$ is 1.*

LEMMA 16. *If $a|b$ and $b|c$ then $a|c$.*

PROOF. By the associative law, $a \cdot \left(\frac{b}{a} \cdot \frac{c}{b}\right) = \left(a \cdot \frac{b}{a}\right) \cdot \frac{c}{b} = b \cdot \frac{c}{b} = c$. □

LEMMA 17 (Units). *$a|b$ iff $(-a)|b$.*

Because of this, we will only consider *positive* divisors.

First problem of factorization.

PROBLEM 18. Find all divisors of a given integer.

This turns out to be really hard. We don't know an efficient way to do this.

1.2.2. The GCD, Two integers. Let $a, b \in \mathbb{Z}$ be non-zero. Let D be the set of common divisors of a and b (non-empty since $1 \in D$). D is bounded since every divisor of a is no larger than $|a|$. Let M be the set of positive common multiples of a, b (non-empty since $|ab| = \pm ab \in M$).

DEFINITION 19. $(a,b) \stackrel{\text{def}}{=} \gcd\{a,b\} = \max D$; $[a,b] \stackrel{\text{def}}{=} \operatorname{lcm}\{a,b\} = \min M$. Also, for all $a \in \mathbb{Z}$, set $(a,0) = a$ and $[a,0] = 0$.

FACT 20. *Every common divisor of a, b divides (a,b). Every common multiple of a, b is divisible by $[a,b]$.*

PROBLEM 21. Given a, b find (a,b) and $[a,b]$.

ALGORITHM 22. *(Naive) Try all elements of the finite sets D, M.*

Entirely impractical since *finding the divisors* is hard. Euclid discussed a much better idea:

LEMMA 23 (Euclid). *Let $a, b \in \mathbb{Z}$. Then $(a,b) = (a-b,b)$.*

PROOF. We prove that both pairs have the same set of common divisors. Indeed, let d divide b. If d also divides a then By Lemma 14 d divides $a-b$. Conversely, if d divides $a-b$ then by that Lemma d divides $a = (a-b)+b$. □

Since $(a,0)=a$ for all a, and since changing the signs of a,b does not change their gcd (why?) we get a method for calculating the gcd of any two integers. For example:

$$\begin{aligned}(24,-153) &= (153,24)\\ &= (129,24)\\ &= (105,24)\\ &= (81,24)\\ &= (57,24)\\ &= (33,24)\\ &= (24,9)\\ &= (15,9)\\ &= (9,6)\\ &= (6,3)\\ &= (3,3)\\ &= (3,0)\\ &= 3\,.\end{aligned}$$

ALGORITHM 24 (Euclid). *Given two integers a,b, output their* gcd*:*

(1) *Replace a with $|a|$, b with $|b|$.*
(2) *If $a<b$ exchange a and b.*
(3) *If $b=0$, terminate and output a.*
(4) *Else, replace a with $a-b$ and go to step 2.*

THEOREM 25. *The algorithm terminates after finitely many steps and outputs the* gcd *of (a,b).*

PROOF. Consider the changes in the quantity $|a|+|b|$ during the course of the algorithm. Every time we reach step 4, we know that $a\geq b>0$. It follows that at the conclusion of step 4, the quantity has decreased by at least $b\geq 1$. Since there is no infinite strictly decreasing sequence of natural numbers (well-ordering), we can reach step 4 only finitely many times. In particular, at some point $b=0$ and we terminate. Finally, by Lemma 23, the replacements and exchanges never change the gcd of the two numbers. □

In fact, more can be said.

CLAIM 26 (Bezout). Every intermediate value considered by Euclid's Algorithm is of the form $xa+yb$ for some $x,y\in\mathbb{Z}$.

PROOF. We prove this by induction on the steps of the algorithm. Certainly this is true at the start, and also changing signs and exchanging a,b doesn't matter. Now assume that at the nth time we reach step 3, we are looking at the numbers $a'=xa+yb>b'=za+wb\geq 0$, where a,b are the initial values and $x,y,z,w\in\mathbb{Z}$. At step 4 we will then replace a' with

$$a'-b'=(x-z)a+(y-w)b$$

which is indeed also of this form, so the situation will hold when we reach step 3 for the $(n+1)$st time. □

We have thus proven (by algorithm) the following fact:

THEOREM 27 (Bezout). *Given $a,b \in \mathbb{Z}$ the exist $x,y \in \mathbb{Z}$ such that $(a,b) = xa+yb$.*

Bezout's theorem admits a direct proof:

PROOF. If $a = b = 0$ there is nothing to prove, so we assume that at least one of a,b is non-zero, and let $I = \{ax+by \mid a,b \in \mathbb{Z}\}$. Note that I is closed under addition and under multiplication by elements of $\mathbb{Z}$: $(ax+by)+q(cx+dy) = (a+qc)x+(b+qd)y \in I$.

By assumption I contains positive numbers (at least one of $|a|$, $|b|$ is positive), so let m be the smallest positive element of I. Every common divisor of a,b divides every element of I; in particular $(a,b) \mid m$. Conversely, we prove that m divides *every* element of I. Since $a,b \in I$ it will follow that m is a common divisor of a,b, hence the greatest common divisor. Let $n \in I$. Dividing with remainder (Theorem 7), we can write $n = qm+r$ for some $0 \leq r < m$ and $q \in \mathbb{Z}$. Then

$$r = n - qm \in I\,.$$

It must be the case that $r = 0$ (else we'd have a positive member of I smaller than m). Then $n = qm$ and m divides n. □

COROLLARY 28. *Every common divisor of a,b divides their GCD.*

PROOF. Let d divide both a,b. Then for any $x,y \in \mathbb{Z}$ $d|xa$ and $d|yb$ so $d|xa+yb$. Now choose x,y so that the $xa+yb = (a,b)$. □

EXERCISE 29. (PS2) If $g = (a,b)$ then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$. Similarly if $(a,c) = 1$ then $(a,bc) = (a,b)$.

1.2.3. The LCM.

DEFINITION 30. Say a,b are *relatively prime* if $(a,b) = 1$.

PROPOSITION 31. *If a,b are relatively prime then $[a,b] = |ab|$.*

PROOF. By Bezout's Theorem there exist x,y such that $xa+yb = 1$. Say that az is also a multiple of b. Then $z = z \cdot 1 = z(xa+yb) = x(az)+(zy)b$ so z is a multiple of b. It follows that az is a multiple of ab, so $|ab|$ is the least positive common multiple. □

LEMMA 32. $[da,db] = d\,[a,b]$.

PROOF. If m is a common multiple of a,b then dm is a common multiple of da,db. Conversely, if m is a common multiple of da,db then m is divisible by d, and $\frac{m}{d}$ is a common multiple of a,b. □

THEOREM 33. *Let a,b be non-zero. Then $(a,b)\,[a,b] = ab$.*

PROOF. We have $[a,b] = \left[(a,b)\frac{a}{(a,b)}, (a,b)\frac{b}{(a,b)}\right] = (a,b)\left[\frac{a}{(a,b)}, \frac{b}{(a,b)}\right] = (a,b)\,\frac{ab}{(a,b)^2}$. □

1.2.4. Sets of integers.

DEFINITION 34. Let S be non-empty finite set of integers. We say that $a \in \mathbb{Z}$ is a *common divisor* of S if a divides every member of S. We say that $a \in \mathbb{Z}$is a *common multiple* of S if it is a multiple of every element of S.

EXAMPLE 35. For any non-empty S, 1 is a common divisor for the elements of S and the products of the elements of S is a multiple of all of them.

DEFINITION 36. Assume that S is finite and has a non-zero member. The *greatest common divisor* of S, written $\gcd(S)$ is the largest integer which is a common divisor of S. The *least common multiple* of S, written $\operatorname{lcm}(S)$ is the smallest positive integer which is a multiple of all elements of S.

NOTATION 37. If $a_1,\ldots,a_k$ are integers we also write $(a_1,\ldots,a_k)$ for their GCD and $[a_1,\ldots,a_k]$ for their LCM.

Note that every common divisor of $\{a_1,\ldots,a_k\}$ is at most $|a_1|$, so only finitely many integers can be the GCD. Similarly, the least common multiple is somewhere between zero and $\prod_{j=1}^{k}|a_j|$.

LEMMA 38. $(a_1,\ldots,a_{k+1}) = ((a_1,\ldots,a_k),a_{k+1})$.

PROOF. Let d be a common divisor of a_{k+1} and $(a_1,\ldots,a_k)$. Then d divides each of $a_1,\ldots,a_k$ (it divides a common divisor of theirs) so $d\,|\,(a_1,\ldots,a_{k+1})$. It follows that $((a_1,\ldots,a_k),a_{k+1})\,|\,(a_1,\ldots,a_{k+1})$. Conversely, let $d=(a_1,\ldots,a_{k+1})$. Then d is a common divisor of $a_1,\ldots,a_k$ so $d\,|\,(a_1,\ldots,a_k)$. Also, $d|a_{k+1}$. It follows that d is a common divisor of both $(a_1,\ldots,a_k),a_{k+1}$ and hence that d divides their GCD, that is that $(a_1,\ldots,a_{k+1})\,|\,((a_1,\ldots,a_k),a_{k+1})$. Now two positive integers that divide each other are equal. □

COROLLARY 39. *Algorithm to find the GCD of a list of numbers.*

1.3. Primes

1.3.1. Irreducibles.

DEFINITION 40. Call $p\in\mathbb{Z}_{>1}$ *prime* if in every factorization $p=ab$, one of a,b is 1.

EXAMPLE 41. 1 has the property, but is specifically excluded. $2,3,5$ are have the property. $4=2\times 2$ doesn't.

THEOREM 42. *Every positive integer can be written as a product of primes.*

PROOF. Let n be the smallest positive integer which cannot be written as a product of positive primes. Then n itself is not irreducible (nor 1), so $n=ab$ with $1<a,b<n$. But then both a,b are product of irreducibles, hence so is n. □

EXAMPLE 43. $60=5\cdot 12=5\cdot 4\cdot 3=5\cdot 2\cdot 2\cdot 3$.

THEOREM 44 (Euclid). *There are infinitely many primes.*

PROOF. Consider $n+1$ where n is the product of all primes. □

REMARK 45. This only shows that there are about $C\log\log x$ primes up to x.

We can rephrase this using an algorithm.

ALGORITHM 46 (Euclid's prime-generating algorithm).
(1) *Set* $P=\{2\}$.
(2) *Let* $n=\prod_{p\in P}$.
(3) *Factor* $n+1$*, and add all its prime divisors to* P.
(4) *Return to step (2).*

By Theorem 42, $n+1$ has prime factor. Since $n,n+1$ are relatively prime, none of these factors belongs to P. It follows that every time around the loop the set P increases, and we eventually obtain infinitely many primes. The first few loops are:

- $P = \{2\}$, $n+1 = 2+1 = 3$.
- $P = \{2,3\}$, $n+1 = 2\cdot 3+1 = 6+1 = 7$.
- $P = \{2,3,7\}$, $n+1 = 6\cdot 7+1 = 42+1 = 43$.
- $P = \{2,3,7,43\}$, $n+1 = 42\cdot 43+1 = 1806+1 = 1807 = 13\cdot 139$.
- $P = \{2,3,7,13,43,139\}$, $n+1 = 1806\cdot 1807+1 = 3,263,443$.
- $P = \{2, 3, 7, 13, 43, 139, 3,263,443\}$, $n+1 = 3,263,442\cdot 3,263,443+1 = 10650056950807 = 547\cdot 607\cdot 1033\cdot 31051$.
- $P = \{2, 3, 7, 13, 43, 139, 547, 607, 1033, 31,051, 3,263,443\}$ and so on

LEMMA 47. *If $n \geq 1$ is reducible, it has a proper factor$\leq \sqrt{n}$.*

PROOF. This is true about any non-trivial factorization. □

COROLLARY 48. *Factorization (and primality testing) by trial division.*

EXAMPLE 49. $126 = 2\cdot 63 = 2\cdot 3\cdot 21 = 2\cdot 3\cdot 3\cdot 7$.

1.3.2. Primes.

THEOREM 50. *Let $p \in \mathbb{Z}_{>1}$ be prime. Then if $p|ab$ then p divides at least one of a,b.*

REMARK 51. This is equivalent to the implication: for all a,b we have $p \nmid a$, $p \nmid b \Rightarrow p \nmid ab$.
It is more natural to remove the requirement that p be positive, but it is not traditional to do so.

EXAMPLE 52. 2 is prime.

PROOF. Assume that a,b are odd. Then there are $k,l \in \mathbb{Z}$ such that $a = 2k+1$, $b = 2l+1$ so $ab = (2k+1)(2l+1) = 2(2kl+k+l)+1$ is also odd. □

EXAMPLE 53. 3 is prime.

PROOF. Let $a,b \in \mathbb{Z}$ not be divisible by 3. Then $a = 3q+r$ and $b = 3q'+r'$ for some $q,q' \in \mathbb{Z}$ and $r,r' \in \mathbb{Z}$ with $1 \leq r,r' < 3$. Then $r,r' \in \{1,2\}$. Since $ab = 3(3qq'+r'q+rq')+rr'$ we have $3 \mid ab$ iff $3|rr'$. But rr' equals one of $1,2,4$ and neither is divisible by 3. □

PROOF OF THEOREM 50. Conversely, let p be a prime which divides the product ab. Assume that $p \nmid a$ and consider the GCD $d = (a,p)$. Since $d|p$, $d = 1$ or $d = p$. Since p does not divide a, $d \neq p$ so $d = 1$. It follows that there exist x,y such that $xp+ya = 1$, at which point

$$b = xpb+yab.$$

Then p divides b since it divides both xpb and yab. □

REMARK 54. Conversely, let p be a number such that $p|ab$ implies $p|a$ or $p|b$. Then either p is a unit or prime. Indeed, if $p = ab$ then p divides one of the factors, so without loss of generality we have $p \mid a$. This forces $|p| \leq |a|$ and hence $|b| \leq 1$. It follows that $|b| = 1$ so b is a unit.

THEOREM 55. *("Fundamental Theorem of Arithmetic") Every positive integer has a factorization into primes, unique up to reordering the factors.*

PROOF. What we need to show is: assume that $n = \prod_{i=1}^{I} p_i = \prod_{j=1}^{J} q_j$ with $\{p_i\}, \{q_j\}$ primes. Then $I = J$ and there is a permutation $\pi \in S_n$ for which $p_i = q_{\pi(i)}$. Let n be the smallest positive integer for which this fails. Let p be a prime divisor of n. Then there is i such that $p_i = p$ and j such that $q_j = p$ ... □

NOTATION 56. We may uniquely write every non-zero integer in the form $n = \varepsilon \prod_p p^{e_p}$ where $\varepsilon \in \{\pm 1\}$ and e_p are non-negative integers, equal to zero for all but finitely many p.

EXAMPLE 57. $v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$.

PROPOSITION 58. *Every positive divisor of $\prod_p p^{e_p}$ is of the form $\prod_p p^{f_p}$ where $0 \le f_p \le e_p$.*

THEOREM 59. $\left(\prod_p p^{e_p}, \prod_p p^{f_p}\right) = \prod_p p^{\min\{e_p, f_p\}}$ *while* $\left[\prod_p p^{e_p}, \prod_p p^{f_p}\right] = \prod_p p^{\max\{e_p, f_p\}}$.

COROLLARY 60. $(a,b)[a,b] = ab$.

PROOF. $\min\{e_p, f_p\} + \max\{e_p, f_p\} = e_p + f_p$. □

1.3.3. Distribution of primes (not examinable).

DEFINITION 61. $\pi(x) = \#\{1 \le p \le x \mid p \text{ prime}\}$.

CONJECTURE 62. *(Gauss circa 1800)* $\lim_{x\to\infty} \pi(x) \cdot \frac{\log}{x} = 1$. *More precisely,* $\pi(x) \sim \mathrm{Li}(x) \stackrel{def}{=} \int_2^x \frac{dt}{\log t}$ *("integers are prime with probability* $\frac{1}{\log t}$*")*

THEOREM 63. *(Chebychev 1850) For all large enough x,*

$$0.9\frac{x}{\log x} \le \pi(x) \le 1.1\frac{x}{\log x}.$$

-

THEOREM 64. *(de la Vallée-Poussin, Hadamard 1896, following Riemann 1859)* $|\pi(x) - \mathrm{Li}(x)| \le Cxe^{-c\sqrt{\log x}}$.

CONJECTURE 65. *(Riemann 1859)* $|\pi(x) - \mathrm{Li}(x)| \le C\sqrt{x}\log x$.

THEOREM 66. *(Dirichlet 1837) Barring local obstruction, every AP contains infinitely many primes.*
(Chebotarev) Let $\pi(q,a;x) = \#\{1 \le p \le x \mid p \equiv a\,(q) \text{ prime}\}$. *Then* $\left|\pi(x) - \frac{1}{\phi(q)}\mathrm{Li}(x)\right| \le Cxe^{-c\sqrt{\log x}}$.

CONJECTURE 67. *(ERH) For* $(a,q) = 1$, $\left|\pi(q,a;x) - \frac{1}{\phi(q)}\mathrm{Li}(x)\right| \le C\sqrt{x}\log x$.

1.3.4. Special primes.

- Twin primes.
- Fermat numbers: $F_n = 2^{2^n} + 1$. Prime for $n = 0,1,2,3,4$. Fermat Conj all prime; Euler showed $641 | 2^{2^{32}} + 1$. No other Fermat primes known.
  - $(F_n, F_m) = 1$ if $n \ne m$, so infinitely many primes.
- Mersenne numbers: $2^p - 1$. Many known; probably there are ∞ many but it is open.
  - Cole, October 1903 meeting of the AMS: $2^{67} - 1 = 193,707,721 \times 761,838,257,287$.
  - Euclid: $2^p - 1$ prime then $2^{p-1}(2^p - 1)$ perfect.
  - Euler: converse.

PROPOSITION 68. $(F_n, F_m) = 1$ *if* $n > m \ge 0$.

PROOF. For any integer x we have

$$\left(x^2+1, x+1\right) = \left((x+1)^2 - 2(x+1) + 2, x+1\right) = (2, x+1)\,.$$

In particular, for $x = 2^{2^m}$ which is even we find $(F_{m+1}, F_m) = 1$. Assume now that $n > m+1$, and for $0 \le j < 2^{n-m-1}$ write $F_{n,j} = 2^{2^n - j2^{m+1}} + 1$ so that $F_{n,0} = F_n$ and $F_{n,2^{n-m-1}-1} = 2^{2^{m+1}} + 1 = F_{m+1}$. Then, for $0 \le j < 2^{n-m-1} - 1$ we have

$$\begin{aligned}
\left(2^{2^n - j2^{m+1}} + 1, 2^{2^m} + 1\right) &= \left(2^{2^n - j2^{m+1}} - 2^{2^m}, 2^{2^m} + 1\right) && \text{Euclid's Lemma} \\
&= \left(2^{2^m}\left(2^{2^n - j2^{m+1} - 2^m} - 1\right), 2^{2^m} + 1\right) && \text{Common factor} \\
&= \left(2^{2^n - j2^{m+1} - 2^m} - 1, 2^{2^m} + 1\right) && \left(2^{2^m}, 2^{2^m} + 1\right) = 1 \\
&= \left(2^{2^n - j2^{m+1} - 2^m} + 2^{2^m}, 2^{2^m} + 1\right) && \text{Euclid's Lemma} \\
&= \left(2^{2^n - j2^{m+1} - 2\cdot 2^m} + 1, 2^{2^m} + 1\right) && \text{Common factor} \\
&= \left(2^{2^n - (j+1)2^{m+1}} + 1, 2^{2^m} + 1\right), &&
\end{aligned}$$

that is $\left(F_{n,j}, F_m\right) = \left(F_{n,j+1}, F_m\right)$. It follows by induction that $(F_n, F_m) = (F_{m+1}, F_m) = 1$. □

COROLLARY 69. *There are infinitely many primes.*

PROOF. No prime divides two of the F_n. □

REMARK 70. Note that this proof only produces n primes up to $2^{2^n} + 1$, i.e. about $\log\log x$ primes up to x.

1.4. Diophantine equations

1.4.1. Diophantine equations.

DEFINITION 71. A *Diophantine equation* is an equation which is to be solved by integers.

REMARK 72. So named because of Diophantus's book.

EXAMPLE 73. Some famous equations include:

(1) Linear equations in one variable: $2x = 6$, $2x = 7$ (encoding divisibility)
(2) Linear equations in two variables: $6x + 5y = 7$, $10x + 7y = 33$ (divisibility plays a major role)
(3) Pythagorean triples: $x^2 + y^2 = z^2$ (such as $3^2 + 4^2 = 5^2$)
(4) Fermat equation: $x^4 + y^4 = z^4$ (Fermat: no solutions except if $xyz = 0$)
(5) Fermat equation: $x^3 + y^3 = z^3$ (Euler: no solutions except if $xyz = 0$)
(6) Fermat equation: $x^p + y^p = z^p$, $p \ge 3$ (Ribet: no solutions assuming the Tanyima–Shimura Conjecture, Wiles: Tanyima–Shimura Conjecture is true).

1.4.2. Linear Diophantine equations.

THEOREM 74. *The set of integral solutions to $ax + by = c$ is as follows:*

(1) *If $a = b = 0$ then the set is empty if $c \neq 0$, all of $\mathbb{Z}^2$ if $c = 0$.*
(2) *Otherwise, let $d = \gcd(a, b)$. Then*

(a) *If $d \nmid c$ the set is empty.*
(b) *If $d \mid c$, let s,t be such that $as+bt=d$. Then the set of solutions is $\left\{\left(\frac{sc}{d}+\frac{b}{d}z, \frac{tc}{d}-\frac{a}{d}z\right)\right\}_{z\in\mathbb{Z}}$.*

REMARK 75. Note that "solving an equation" requires doing two things: showing that every solution is in the set, and showing that every member of the set is a solution.

EXAMPLE 76. The equation $5x+11y=7$ has the solutions $\{(-14+11k, 7-5k)\}_{k\in\mathbb{Z}} = (-14,7)+(11,-5)\mathbb{Z}$. The equation $10x+22y=9$ has no solutions. The equation $10x+22y=14$ has the same solutions as $5x+11y=7$.

PROOF. The first part is obvious. For the second, certainly $d=\gcd(a,b)$ divides any integer of the form $ax+by$ so if the equation has solutions we must have $d|c$. Conversely, suppose $d|c$. We can then study the equation $\frac{a}{d}x+\frac{b}{d}y=\frac{c}{d}$, where now $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$. □

- Example: $10x+7y=33$

REMARK 77. Linear equations will recur in several guises; they are common.

1.4.3. Non-linear equations: finding all Pythagorean triples.

REMARK 78. The main motivation for this section is not the "bottom line" result, but rather the *techniques* used along the way.

Let $x,y,z\in\mathbb{Z}$ satisfy $x^2+y^2=z^2$. What can we say about them?
Step 0: Signs. If $x=0$ then the equation is $y^2=z^2$ with solutions $y=\pm z$. Also, changing the sign of x, say, does not affect x^2.

CONCLUSION. We may assume x,y,z are strictly positive.

Step 1: Removing common factors. Suppose a prime p divides both of x,y. Then $p|x^2+y^2$ so $p|z^2$. But this means $p|z\cdot z$ so $p|z$ or $p|z$, that is $p|z$. But now p divides all three of x,y,z and then dividing the equation by p^2 we get:

$$\left(\frac{x}{p}\right)^2+\left(\frac{y}{p}\right)^2=\left(\frac{z}{p}\right)^2.$$

Dividing by common factors whenever we can, we can eventually write $x=d\cdot x'$, $y=d\cdot y'$, $z=d\cdot z'$ so that

$$x'^2+y'^2=z'^2.$$

CONCLUSION. For the next steps we may assume that x,y,z are *pairwise relatively prime*.

Step 2: Congruence considerations. Since x,y do not have a common prime divisor, at most one of them is even, so at least of them is odd. Can *both* be odd?

FACT 79 (PS2). *Let $x\in\mathbb{Z}$. If x is even, x^2 is divisible by 4. If x is odd, x^2 leaves remainder 1 when divided by 4.*

It's also clear that if z is even, z^2 is a multiple of 4. Suppose now that x,y were both odd. Then $x^2=1+4q$ for some q, $y^2=1+4r$ for some r, but then $z^2=x^2+y^2=2+4(r+q)$ would leave remainder 2 when divided by 4 and this is forbidden.

CONCLUSION. One of x,y is even and one is odd. Wlog x is odd and y is even. Then x^2 is odd, y^2 is even, so z^2 is odd, so x,z are odd.

Step 2: Factoring the equation. Rewrite the equation as:

$$y^2 = z^2 - x^2 = (z+x)(z-x).$$

As in step 1 we begin by trying to remove common factors. We note that $y, z+x, z-x$ are all even (x, z are both odd) so we can immediately divide by 4 and write

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right). \tag{1.4.1}$$

QUESTION. *Can there be more common factors?*

Answer: No. (Trick: polarization) Suppose$p$ divides both of $\frac{z+x}{2}$ and $\frac{z-x}{2}$. Then p divides their sum and their difference. This means

$$\begin{aligned} p \quad | \quad z &= \frac{z+x}{2} + \frac{z-x}{2} \\ p \quad | \quad x &= \frac{z+x}{2} - \frac{z-x}{2}. \end{aligned}$$

But x, z have no common factors.

CONCLUSION. In the factorization (1.4.1) the factors on the right are relatively prime.

Step 3: Unique factorization. Let $u = \frac{z+x}{2}$, $v = \frac{z-x}{2}$ and we know that $uv = \left(\frac{y}{2}\right)^2$ is a square.

LEMMA 80. *Let $n \in \mathbb{Z}_{>0}$ have the prime factorization $n = \prod_p p^{e_p}$. Then n is a square iff all e_p are even.*

PROOF. Suppose $n = m^2$ and let the factorization of m be $m = \prod_p p^{f_p}$. Then $n = m^2 = \prod_p p^{2f_p}$. Conversely, suppose each e_p is even. Then $n = m^2$ where $m = \prod_p p^{(e_p/2)}$. □

LEMMA 81. *Suppose u, v are relatively prime integers such as uv is a square. Then both of u, v are squares.*

PROOF. Let the prime factorizations of u, v be

$$\begin{aligned} u &= \prod_{i=1}^{r} p_i^{e_i} \\ v &= \prod_{j=1}^{s} q_j^{f_j} \end{aligned}$$

with all $e_i, f_j > 0$. Since u, v are relatively prime, no p_i equals any q_j. The prime factorization of uv is then

$$uv = \prod_{i=1}^{r} p_i^{e_i} \prod_{j=1}^{s} q_j^{f_j}$$

with all the primes appearing distinct. By the previous Lemma, if uv is a square than each e_i and f_j is even. But since each e_i is even u is a square, and since each f_j is even v is a square. □

CONCLUSION. Both $\frac{z+x}{2}$ and $\frac{z-x}{2}$ are squares.

Step 4: Parametrization. Accordingly, let $\frac{z+x}{2} = n^2$ and let $\frac{z-x}{2} = m^2$. The numbers m,n are relatively prime, since their squares $\frac{z+x}{2}$ and $\frac{z-x}{2}$ are. Also, their sum z is odd so they have opposite parities. Noting that $\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = m^2n^2$ we get:

$$\begin{aligned} x &= \frac{z+x}{2} - \frac{z-x}{2} = n^2 - m^2 \\ y &= 2mn \\ z &= \frac{z+x}{2} + \frac{z-x}{2} = n^2 + m^2 \end{aligned}$$

Step 5: Solution. Recalling the common factor construction of step 1, we have shown:

PROPOSITION 82. *Let x,y,z satisfy $x^2+y^2=z^2$ where $x,y,z>0$. Then (up to swiching x,y) there are $m,n,d>0$ with m,n relatively prime and not both odd so that*

$$\begin{cases} x = & d\cdot\left(n^2-m^2\right) \\ y = & d\cdot 2nm \\ z = & d\cdot\left(n^2+m^2\right). \end{cases}$$

QUESTION 83. *Are we done?*

Answer: No – we need to check these are solutions.

LEMMA 84. *All of these are indeed solutions to the equations.*

PROOF. The following is an algebraic identity:

$$\left(d\cdot\left(n^2-m^2\right)\right)^2 + (d\cdot 2mn)^2 = \left(d\cdot\left(n^2+m^2\right)\right)^2$$

□

CHAPTER 2

Congruences

2.1. Motivation

Consider the linear congruence $10x+7y=33$. We already know that its solutions are

$$\left\{\begin{pmatrix}-66\\99\end{pmatrix}+\begin{pmatrix}7\\-10\end{pmatrix}k\right\}.$$

We now take a different point of view. We write the equation as

$$10x+\begin{pmatrix}\text{multiple}\\\text{of } 7\end{pmatrix}=33$$

(leaving y as an *implicit* variable). We can similarly write the solution as:

$$x=-66+\begin{pmatrix}\text{multiple}\\\text{of } 7\end{pmatrix}.$$

The equation now seems like an equation in *one* unknown, and seems to have *one solution*.

2.2. Arithmetic in congruences

2.2.1. Examples: arithmetic mod $2,3,4$.

- Construct addition and multiplication tables mod $2,3,4$
- Observe we only need the *reduced residues* $\{0,1\}$, $\{0,1,2\}$, $\{0,1,2,3\}$.
- Observe usual rules of arithmetic (for addition and multiplication) still hold
- Observe

2.2.2. Formal proofs.

DEFINITION 85. For $a,b,m\in\mathbb{Z}$ with $m\geq 2$, $a\equiv b\,(m)$ iff $m\mid a-b$.

REMARK 86. Informally, $a\equiv b\,(m)$ means "$a=b$ up to a multiple of m".

LEMMA 87 ("implicit variable"). *$a\equiv b\,(m)$ iff there is $k\in\mathbb{Z}$ such that $a-b=km$ or $a=b+km$.*

PROPOSITION 88. *Congruence mod m is an equivalence relation.*

THEOREM 89 (Arithmetic). *If $a\equiv a',b\equiv b'\,(m)$ then*

$$a\pm b\equiv a'+b'\,(m)$$

and

$$ab\equiv a'b'\,(m).$$

PROOF. Say $a'=a+km$, $b'=b+lm$. Then $a'\pm b'=a\pm b+(k\pm l)m$ and $a'b'=ab+(al+bk+kl)m$. □

FACT 90 (Division Thm). *Every congruence class mod m contains a unique representative $0 \leq r < m$.*

DEFINITION 91. The *reduction* of a mod m is that $0 \leq r < m$ which is congruent to a.

EXAMPLE 92. (Divisibility tests) $m \mid a$ iff the reduction of a mod m is zero.

2.3. Application: Divisibility tests

Write an integer $n \in \mathbb{Z}_{\geq 1}$ using its decimal expansion: $n = \sum_{i=0}^{d} a_i 10^i$ where the *digits* $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$. What can we tell about n knowing only its digits?

LEMMA 93 (Divisibility by $2,5,10$). *$n \equiv a_0 \,(10)$, hence also $n \equiv a_0 \,(5)$ and $n \equiv a_0 \,(2)$.*

PROOF. We have $10^0 = 1$ and for $i \geq 1$, $10^i = 10 \cdot 10^{i-1} \equiv 0 \,(10)$. It follows that

$$n = \sum_{i=0}^{d} a_i 10^i \equiv a_0 + \sum_{i=1}^{d} a_i \cdot 0 \equiv a_0 \,(10)\,.$$

□

What about divisibility by 9?

LEMMA 94. *For all $k \geq 0$, $10^k \equiv 1 \,(9)$ (proof by induction)*

PROPOSITION 95 (Divisibility by 9). *For all $n \geq 0$, $n \equiv S(n) \,(9)$ where $S(n)$ is the* digit sum *of n.*

PROOF. We have

$$n = \sum_{i=0}^{d} a_i 10^i \equiv \sum_{i=0}^{d} a_i \cdot 1 \equiv S(n) \,(9)\,.$$

□

LEMMA 96. *If $n > 9$ then $S(n) < n$.*

PROOF. $n - S(n) = \sum_{i=1}^{d} a_i \left(10^i - 1\right) > 0$ as long there is $i \geq 1$ with $a_i > 0$. □

ALGORITHM 97. *To reduce n mod 9 keep replacing n with $S(n)$ until the resulting number (*"digital root"*) is at most 9.*

COROLLARY 98. *n is divisible by 9 iff its digital root is 9, by 3 iff its digital root is $3,6$ or 9.*

EXERCISE 99. (PS3) Construct a similar test for divisibility by 11, using $10 \equiv -1 \,(11)$.

2.4. Negatives, inverses and linear equations

We'd like to solve equations like $ax + b \equiv c \,(m)$. For this we need to be able to:

- Subtract b
- Divide by a

2.4.1. The negative (reinforces reduced residue).

- "Residue class" or "congruence class" = all numbers congruent to a given number, equivalently all numbers giving the same reminder (mod m)
- "Reducing" an integer mod m = replacing with the reduced residue, the remainder upon division by m.
- Let a be a reduced residue. What is the reduction of $-a$?
  - It is $m-a$.
- This allows us to solve the equation $x+a \equiv b\,(m)$.

2.4.2. The modular inverse.

DEFINITION 100. Say that b is a *modular inverse* of a (mod m) if $ab \equiv 1\,(m)$. Say that a is *invertible* if it has a modular inverse.

PROPOSITION 101. *a is invertible* mod m *iff* $(a,m)=1$.

PROOF. Assume that $ab \equiv 1\,(m)$. Then $1 = ab+km$. Thus any prime dividing both a and m must divide 1. Conversely, let a,m be relatively prime. By Bezout's Theorem 27, there are x,y such that $ax+my=1$, which means that $ax \equiv 1\,(m)$. □

LEMMA 102. *The modular inverse is unique (if it exists)*

PROOF. Suppose b,b' are both modular inverses of a. Then $ab' \equiv 1\,(m)$. Multiplying both sides by b we conclude $b \equiv b\cdot 1 \equiv b\cdot(ab') \equiv (ba)b' \equiv 1\cdot b' \equiv b'\,(m)$. □

NOTATION 103. Write $\bar{a}$ for the modular inverse of a (when m is understood from context).

EXAMPLE 104 (Euler). $5\cdot 128 = 640 = 641-1$ so $2^7 \equiv -\bar{5}\,(641)$. Also, $641 = 625+16$ so $2^4 \equiv -5^4\,(641)$. We conclude that $2^{32}+1 = 2^4\left(2^7\right)^4+1 \equiv -5^4\left(-\bar{5}\right)^4+1 \equiv -1\left(5\cdot\bar{5}\right)^4+1 \equiv 0\,(641)$. In fact, $2^{32}+1 = 641\cdot 6,700,417$.

PROPOSITION 105. *a is a zero-divisor iff* $(m,a)>1$.

PROOF. Let $d=(m,a)$. If $d>1$ then Then $1 \le \frac{m}{d} < m$ so $\frac{m}{d} \not\equiv 0\,(m)$. Also, $a\cdot\frac{m}{d} = \left(\frac{a}{d}\cdot d\right)\cdot\frac{m}{d} = \frac{a}{d}\cdot\left(d\cdot\frac{m}{d}\right) = \frac{a}{d}\cdot m \equiv \frac{a}{d}\cdot 0 \equiv 0\,(m)$. If $d=1$ then a is invertible. Suppose that $ab \equiv 0\,(m)$. Then $b = 1\cdot b \equiv (\bar{a}a)b \equiv \bar{a}(ab) \equiv \bar{a}\cdot 0 \equiv 0\,(m)$. □

2.4.3. Linear equations.

THEOREM 106. *Consider the congruence $ax \equiv b\,(m)$, and let $d=(a,m)$. If $d \nmid b$ there are no solutions. Otherwise it is equivalent to the congruence $\frac{a}{d}x \equiv \frac{b}{d}\,(\frac{m}{d})$. If $(a,m)=1$ then $ax \equiv b$ iff $x \equiv \bar{a}b$.*

REMARK 107. Every class mod $\frac{m}{d}$ splits into d classes mod m – and we expect the final answer to be in terms of classes mod m.

2.4.4. Linear equations: several variables. Same techniques as for usual linear algebra. For example we'll solve

$$\begin{cases} 5x+2y & \equiv 3\,(12) \\ 2x+7y & \equiv 5\,(12) \end{cases}$$

2.5. The CRT

2.5.1. Example: a non-linear congruence. Suppose we want to solve $x^2 \equiv 1\,(7)$. This is not hard because we can factor:

$$x^2-1 \equiv 0\,(7) \iff 7 \mid x^2-1 \iff 7 \mid (x-1)(x+1) \iff 7|(x-1) \vee 7|(x+1) \iff x \equiv \pm 1\,(7).$$

Same if 7 is replaced by any prime ("quadratic equation should have two solutions"). What about mod 35? Obvious solutions ± 1 but note also that $6^2 = 36 \equiv 1\,(35)$ while $6 \not\equiv \pm 1$. How can we find such solutions?

- Factor $35 = 5 \cdot 7$.
- Solve congruence mod 5 and mod 7 separately.
- Put solutions together.

2.5.2. Formal statement.

THEOREM 108 (CRT). *Let $\{m_j\}_{j=1}^J$ be pairwise relatively prime, and let $M = \prod_j m_j$. Let $\{a_j\}_{j=1}^J \subset \mathbb{Z}$. Then there is $a \in \mathbb{Z}$, unique mod M, such that $a \equiv a_j\,(m_j)$.*

PROOF. Assume first that $a_1 = 1$ and that $a_j = 0$ for $2 \le j \le J$. Let $N = \prod_{j=2}^J m_j$ so that $M = m_1 N$. It is then enough to find a such that $a \equiv 1\,(m_1)$ while $a \equiv 0\,(N)$. Since $(N, m_1) = 1$ can take $a = N\bar{N}$ where $\bar{N}$ is any inverse of N mod m_1. It follows that there exist $\{y_j\}_{j=1}^J$ such that $y_i \equiv \delta_{ij}\,(m_j)$. For existence set $a = \sum_j y_j a_j$. For uniqueness by subtraction it is enough to consider the case $a \equiv 0\,(m_j)$ for all j, for which a must be divisible by M. □

EXAMPLE 109. Divide the six residue classes mod 6 into their classes mod 2 and 3.

2.5.3. Summary.

(1) Let $M = m_1 m_2$. Then
   (a) The residue class of a mod M is contained in the residue class of a mod m_1.
   (b) The residue class of a mod m_1 splits into m_2 classes mod M: the classes of $a, a + m_1, a + 2m_1, a + 3m_1, \ldots, a + (m_2 - 1)m_1$.
   (c) The residue class of

(2) In general let $M = m_1 m_2 \cdots m_r$.
   (a) For each i let $N_i = \frac{M}{m_i}$, in other words $N_i = \prod_{j \neq i} m_j$. Use Euclid's Algorithm to find x_i, y_i such that $N_i x_i + m_i y_i = 1$ and let $b_i = N_i x_i$.
   (b) Given $\{a_i\}_{i=1}^r$ set $a = \sum_{i=1}^r a_i b_i$.

EXAMPLE 110. Solve $x \equiv 1\,(3)$, $x \equiv 2\,(5)$ and $x \equiv 3\,(7)$. Indeed $35 \cdot 2 = 70 \equiv 1\,(3)$, $21 \equiv 1\,(5)$ and $15 \equiv 1\,(7)$. It follows that the solution is $x \equiv 70 \cdot 1 + 21 \cdot 2 + 15 \cdot 3\,(3 \cdot 5 \cdot 7)$, that is $x \equiv 157 \equiv 52\,(105)$.

2.6. The multiplicative group

2.6.1. Wilson's Theorem.

THEOREM 111. *Let p be prime. Then $(p-1)! \equiv -1\,(p)$.*

PROOF. This is exactly the product of all residues mod p. We can pair each residue with its inverse, except for -1 which is its own inverse. □

EXAMPLE 112. What is 6! mod 7.

2.6.2. Multiplicative order. Examine powers of 2 mod 7, mod 11. Powers of 5 mod 11 and see periodicity. Examine powers of 2 mod 6 and see periodicity but no 1.

DEFINITION 113. For $(a,m)=1$ the *multiplicative order of a mod m is* $\operatorname{ord}_m(a)=\min\{n\geq 1 \mid a^n\equiv 1\,(m)\}$.

PROPOSITION 114. *Let* $(a,m)=1$.
Then $a^r\equiv a^s\,(m)$ *iff* $r\equiv s\,(\operatorname{ord}_m(a))$.

PROOF. Wlog $r=s+t$ for $t\geq 0$. Suppose first that $r\equiv s\,(\operatorname{ord}_m(a))$, that is $\operatorname{ord}_m(a)\mid t$. Then

$$a^r=a^sa^t=a^s\cdot a^{\operatorname{ord}_m(s)\frac{t}{\operatorname{ord}_m(s)}}=a^s\left(a^{\operatorname{ord}_m(s)}\right)^{\frac{t}{\operatorname{ord}_m(s)}}\equiv a^s1^{\frac{t}{\operatorname{ord}_m(s)}}\equiv a^s\,(m).$$

Conversely, suppose $a^r\equiv a^s\,(m)$. Multiplying both sides by $\bar{a}^s$ we get

$$a^t=a^{r-s}\equiv a^r\bar{a}^s\equiv a^s\bar{a}^s\equiv(a\bar{a})^s\equiv 1\,(m).$$

By the division theorem we can write $t=q\operatorname{ord}_m(a)+u$ for some $u<\operatorname{ord}_m(a)$. Then

$$1\equiv a^t\equiv\left(a^{\operatorname{ord}_m(a)}\right)^q a^u\equiv a^u\,(m).$$

If u is positive this contadicts the minimality of $\operatorname{ord}_m(a)$, so $u=0$ and $\operatorname{ord}_m(a)\mid t=r-s$. □

EXAMPLE 115. The order of 2 mod 2^n-1 is n: it divides n since $2^n\equiv 1\,(2^n-1)$ but can't be smaller.

What can we say about the multiplicative order?

2.6.3. Fermat's Little Theorem.

THEOREM 116 (Fermat). *Let p be prime, and let $p\nmid a$. Then* $a^{p-1}\equiv 1\,(p)$.

PROOF 1. Let

$$A=(p-1)!=\prod_{x\,(p)}{}'\,x.$$

Now multiply both sides by a^{p-1}. We get:

$$a^{p-1}\cdot A=\prod_{x\,(p)}{}'\,(ax)=\prod_{y\,(p)}y=A$$

since multiplication by a is a bijection of the invertible residues with themselves. Multiplying by $\bar{A}$ we get $a^{p-1}\equiv 1\,(p)$. □

REMARK 117. The "correct" proof is via Lagrange's Theorem in group theory; see Math 322.

EXAMPLE 118. 35 is not prime since $2^{34}\not\equiv 1\,(35)$.

- $2^{10}=1024=1023+1\equiv 1\,(341)$. It follows that $2^{340}\equiv 1\,(341)$. But $11\mid 341$ (why?) so this is not a prime.
- What is the order of a mod 23? It must divide $23-1=22=2\cdot 11$ so it is either 1, 2, 11, or 22.
  - Only ± 1 have order dividing 2.
  - Order 11 if a is a square.
  - Later: iff a is a square, and can quickly determine whether a is a square or not.

DEFINITION 119. Call p a *Sophie Germain prime* if $2p+1$ is also prime. In that case call $q = 2p+1$ a *safe* prime.

LEMMA 120. *Let $q = 2p+1$ be a safe prime. Let $a \not\equiv -1, 0, 1\,(q)$. Then the order of a mod q is either p or $2p$.*

2.6.4. Euler's Theorem.

DEFINITION 121. $\phi(m) = \#U(m)$

EXAMPLE 122. $\phi(p) = p-1$, $\phi(27) = 27 - \frac{1}{3}\cdot 27 = 18$.

THEOREM 123 (Euler). *For any m, $a^{\phi(m)} \equiv 1\,(m)$.*

2.6.5. Primality testing. Pseudoprimes, Charmichael numbers.
Aside: Miller's algorithm and Rabin's version.

ALGORITHM 124. *Modular exponentiation by repeated squaring*

CHAPTER 3

Arithmetic functions

3.1. Dirichlet convolution

DEFINITION 125. An *arithmetical function* is a function $f\colon \mathbb{Z}_{\geq 1} \to \mathbb{R}$ (more generally, to $\mathbb{C}$).

EXAMPLE 126. Some standard functions.

- All-ones function $I(n) = 1$, *identity function* $N(n) = n$, *delta-function* $\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$.
- *Characteristic function of the primes*: $P(n) = \begin{cases} 1 & n \text{ prime} \\ 0 & \text{not} \end{cases}$ for which $\pi(x) = \sum_{n \leq x} P(n)$.

  The *von-Mangoldt function* $\Lambda(n) = \begin{cases} \log p & n = p^k, k \geq 1 \\ 0 & \text{else} \end{cases}$ which is the "right way" to count primes using *Chebychev's function* $\psi(x) = \sum_{n \leq x} \Lambda(n)$.
- Let $n = \prod_p p^{e_p}$. Then $\omega(n) = \#\{p \text{ prime} : p|n\}$, $\Omega(n) = \sum_p e_p$. From these get the *Möbius function* $\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \text{ squarefree} \\ 0 & \text{else} \end{cases}$, the *Liouville function* $\lambda(n) = (-1)^{\Omega(n)}$.
- $\phi(n) = \#\{0 \leq a < n \mid (a,n) = 1\}$, $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$, $\sigma_k(n) = \sum_{d|n} d^k$.

DEFINITION 127. Call f *multiplicative* if $f(mn) = f(m)f(n)$ if $(m,n) = 1$.

REMARK 128. This usually has to do with the CRT.

EXAMPLE 129. $\phi(n)$ is multiplicative (proof later).

LEMMA 130. *If f is multiplicative and $f(1) \neq 1$ then $f(n) = 0$ for all n.*

PROOF. $f(n) = f(n \cdot 1) = f(n)f(1)$ so $(1 - f(1)) \cdot f(n) = 0$ for all n. □

PROPOSITION 131. *f multiplicative and $n = \prod_p p^{e_p}$ then $f(n) = \prod_p f(p^{e_p})$.*

PROOF. Induction on number of prime factors of n. □

COROLLARY 132. $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ *so* $\phi(\prod_p p^{e_p}) = \prod_{p|n}\left(p^{e_p} - p^{e_p - 1}\right) = \prod_{p|n} p^{e_p}\left(1 - \frac{1}{p}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$.

DEFINITION 133. f is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all n.

EXAMPLE 134. $I(n)$, $\delta(n)$, $N^k(n)$.

DEFINITION 135. The *Dirichlet convolution* of f, g is the arithmetical function

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{de=n} f(d)g(e)$$

The second definition shows that $f*g = g*f$. By convention the sum is over positive divisors and factorizations only.

EXAMPLE 136. Calculate $(\phi * I)(n)$ for small values of n, note that $\phi * I = N$.

THEOREM 137. $\phi * I = N$.

PROOF. (Textbook) Combinatorial – $\sum_{d|n} \phi(\frac{n}{d}) = n$ since this counts the integers between $1, n$ according to their gcd with n. □

THEOREM 138. *f, g multiplicative then so if $f*g$.*

PROOF. Let $\gcd(m_1, m_2) = 1$. Then there is a bijection between divisors $d|m_1m_2$ and pairs $d_1|m_1$, $d_2|m_2$ by $(d_1, d_2) \mapsto d_1d_2$ and $d \mapsto (\gcd(d, m_1), \gcd(d, m_2))$. It follows that

$$\begin{aligned}
(f*g)(m_1m_2) &\overset{\text{def}}{=} \sum_{d|m_1m_2} f(d)g(\frac{m_1m_2}{d}) \\
&= \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1d_2)g\left(\frac{m_1}{d_1} \cdot \frac{m_2}{d_2}\right) \\
&= \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1)f(d_2)g\left(\frac{m_1}{d_1}\right) g\left(\frac{m_2}{d_2}\right) \qquad f, g \text{ multiplicative} \\
&= \sum_{d_1|m_1} f(d_1)g\left(\frac{m_1}{d_1}\right) \sum_{d_2|m_2} f(d_2)g\left(\frac{m_2}{d_2}\right) \\
&= ((f*g)(m_1)) \cdot ((f*g)(m_2)) \,.
\end{aligned}$$

□

EXAMPLE 139. $\tau = I*I$, $\sigma_k = I*N^k$.

REMARK 140. f, g completely multiplicative doesn't mean $f*g$ is so, e.g. $\tau = I*I$.

EXAMPLE 141. $\tau(p^k) = k+1$ so $\tau(\prod_p p^{e_p}) = \prod_p (e_p+1)$. $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$ so $\sigma(\prod_p p^{e_p}) = \prod_{p|n} \frac{p^{e_p+1}-1}{p-1}$.

PROBLEM 142. (Past final) $\tau(n) = 77$ and $6|n$. Find n.

3.2. Mersenne primes and perfect numbers

DEFINITION 143. (cf PS1) Call n *deficient* if $\sigma(n) < 2n$, *abundant* if $\sigma(n) > 2n$ and *perfect* if $\sigma(n) = 2n$.

EXAMPLE 144. $6, 28$.

Not clear if odd perfect numbers exist. We'll study even perfect numbers.

- Let $n = 2^s m$ be perfect with m odd. Then by multiplicativity $\sigma(n) = \sigma(2^s)\sigma(m) = \left(2^{s+1}-1\right)\sigma(m)$.
  - We used $(2^s, m) = 1$. Not enough to say "2^s even, m odd".
- By assumption also $\sigma(n) = 2n = 2^{s+1}m$. It follows that $2^{s+1} | \left(2^{s+1}-1\right)m$. Since $\left(2^{s+1}, 2^{s+1}-1\right) = 1$ (they are consecutive) we have $2^{s+1}|\sigma(m)$ so write $\sigma(m) = 2^{s+1}t$.

- We then have $2^{s+1}m = \left(2^{s+1}-1\right)2^{s+1}t$ that is $m = \left(2^{s+1}-1\right)t$.
- If $t > 1$ then $1, t, \left(2^{s+1}-1\right)t$ are distinct divisors of m so $\sigma(m) \geq 1 + t + \left(2^{s+1}-1\right)t = 1 + 2^{s+1}t > \sigma(m)$, a contradiction.
- It follows that $m = 2^{s+1}-1$ and that $\sigma(m) = 2^{s+1} = m+1$. In particular, m has no other divisors that $1, m$ so m is prime.
- By PS2, if $2^{s+1}-1$ is prime then $s+1$ itself is prime. We have shown that every even perfect number is of the form $2^{p-1}(2^p-1)$ where $p, 2^p-1$ are both prime.
- Conversely, if $p, 2^p-1$ are both prime then $\sigma\left(2^{p-1}(2^p-1)\right) = \sigma\left(2^{p-1}\right)\sigma(2^p-1) = (2^p-1)(1+2^p-1) = 2\cdot 2^{p-1}(2^p-1)$.

THEOREM 145. *An even number is perfect iff it is of the form $2^{p-1}(2^p-1)$ for a prime of the form 2^p-1.*

DEFINITION 146. The numbers of the form $M_n = 2^n - 1$ are called *Mersenne numbers*.

PROPOSITION 147. *Let q, p be primes with $q|2^p-1$. Then $q \equiv 1\,(p)$.*

PROOF. PS5 □

EXAMPLE 148. The first few Mersenne primes and associated perfect numbers are:

- $2^2-1 = 3$; $2^1\cdot 3 = 6$
- $2^3-1 = 7$; $2^2\cdot 7 = 28$
- $2^5-1 = 31$ – if not prime would have a prime divisor$\equiv 1\,(5)$ and $< 6 = \sqrt{36}$ which is impossible. The perfect number is $2^4\cdot 31 = 496$.
- $2^7-1 = 127$ – if not prime would have a prime divisor $\equiv 1\,(7)$ and $< 12 = \sqrt{144}$ but there are no such primes. $2^6\cdot 127 = 8128$.

EXAMPLE 149. $2^{11}-1 = 2047$ – if not prime would have a prime divisor $\equiv 1\,(11)$ and $< 50 = \sqrt{2500}$. The only prime in this range is 23 and indeed $\frac{2047}{23} = 89$.

CHAPTER 4

Cryptology

4.1. Introduction

- Three parties: A (Alice) would like to communicate some message P ("plaintext") to B (Bob). The eavesdropper Eve will know everything Alice sends.
- Alice and Bob will agree on a pair of functions E ("encryption"), D ("decryption") such that $D(E(P)) = P$ for all P. Alice will send the *ciphertext* $C = E(P)$. Bob will recover the plaintext by evaluating $P = D(C)$.
  - "Symmetric crypto": Alice and Bob keep D, E secret. Eve only knows C and has to guess what D, E are.
  - "Public-key / Asymmetric crypto": Eve knows both C and the function E, while Bob's function D is kept secret.
- The first scheme requires prior communication between Alice and Bob (to agree on the functions). Usually this prior communication is facilitated by a method of the second kind.
  - PKC is more involved, more computationally expensive. Usually only used for key exchange after which a symmetric cipher is used.
- Alice and Bob do "cryptography" (create methods of communications); Eve does "cryptanalysis" (breaking such methods).

4.2. Character and block ciphers

In a *character cipher* we encode every letter of the message as an integer $P \in \{0, \dots, 25\}$ (thought of as residues mod 26). The function D, E are then maps $\{0, \dots, 25\} \to \{0, \dots, 25\}$.

EXAMPLE 150. (Caesar cipher) $E(P) \equiv P + 3\,(26)$ so $D(C) = C - 3\,(26)$.

- HELLO + 3 = , decrypt by -3.

EXAMPLE 151. (Affine cipher) $E(P) = aP + b\,(26)$.

- Must have *a invertible* mod 26 for this to make sense.
- In that case $D(C) \equiv \bar{a}(C - b) = \bar{a}C - \bar{a}b$ is also an affine function
- HELLO via $\cdot 3 - 7$, decrypt via $\cdot 9 + 63 = \cdot 9 + 11$.

REMARK 152. (ETAOIN) Character ciphers are very weak, since they preserve the *frequency distribution* of the letters (which is highly non-uniform). They also preserve the *order* of the letters (TH most common digraph, THE most common trigraph).

Even if a different substitution is used for different plaintext letters, but the sequence of substitutions repeat it's possible to recover the block length by checking the letter distributions in residue classes.

Block ciphers: work with several letters are once, perhaps on a rolling basis. E.g. affine-linear map on the vector coming from several letters.

4.3. Asymmetric encryption: RSA

CHAPTER 5

Primitive roots

5.1. Primitive roots

PROBLEM 153. Solve $x^5 \equiv 7\,(17)$.

Find $\mathrm{ord}_{17}(2) = 8$ and $6^2 \equiv 2$ so $\mathrm{ord}_{17}(6) = 16$. Now take log base 16. Similarly for $x^5 \equiv 4$ and $x^6 \equiv 4$.

DEFINITION 154. For $(a,m) = 1$ set $\mathrm{ord}_m(a) = \min\{n \geq 1 \mid a^n \equiv 1\,(m)\}$

Call r a *primitive root* mod p if $\mathrm{ord}_p(r) = \phi(m)$.

EXAMPLE 155. Mod 17. Mod 19.

LEMMA 156. *a is a primitive root iff every invertible residue is a power of a; in this case the invertible residues are given by $\left\{a^j\right\}_{j=0}^{\phi(m)-1}$.*

THEOREM 157. *("Discerte Logarithm") Let r be a primitive root mod m. Then the equation $x^n \equiv r^l\,(m)$ has solutions iff $(n,\phi(m))|l$ in which case there are $(n,\phi(m))$ such solutions.*

In particular, b is an nth power mod m iff $b^{\frac{\phi(m)}{(n,\phi(m))}} \equiv 1\,(m)$, in which case it has $(n,\phi(m))$ nth roots.

PROOF. Changing variables to $x = r^t$ we need to solve $nt \equiv l\,(\phi(m))$ which is a linear congruence. □

THEOREM 158. *There is a primitive root mod m iff m is of the form $2,4,p^k,2p^k$ where p is an odd prime and $k \geq 1$.*

5.2. Primitive roots mod p

Fix a prime p.

Two key ingredients:

PROPOSITION 159. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n mod p (that is, $p \nmid a_n$). Then the congruence $f(x) \equiv 0\,(p)$ has at most n solutions.*

PROOF. If $f(a) \equiv 0\,(p)$ then $x - a$ divides f mod p, and continue by induction. □

PROPOSITION 160. $\sum_{d|n} \phi(d) = n$.

THEOREM 161. *For every $d|p-1$ there are at d elements of order dividing d, and $\phi(d)$ elements of order exactly d.*

PROOF. There are at most d elements since x has order dividing n iff $x^d \equiv 1\,(p)$. Let $A_d = \left\{1 \leq a \leq p-1 \mid \mathrm{ord}_p(a) = d\right\}$. If this set is not empty let $a \in A_d$. Then $\left\{a^j\right\}_{j=0}^{d-1}$ are all distinct

so these are all elements of order dividing d. Since $\mathrm{ord}_p(a^j) = \frac{\mathrm{ord}_p(a)}{(j,\mathrm{ord}_p(a))}$, exactly $\phi(d)$ of these elements are of order d exactly. It follows that $\#A_d \le \phi(d)$. Thus:

$$p-1 = \#\{1 \le a \le p-1\} = \#\left(\cup_{d|p-1} A_d\right) \le \sum_{d|p-1} \#A_d \le \sum_{d|p-1} \phi(d) = p-1\,.$$

It follows that we must have equalities throughout, that is that $\#A_d = \phi(d)$. In particular for $n|p-1$, the elements of order dividing n are $\cup_{d|n} A_d$ and there are $\sum_{d|n}\phi(d) = n$ of them. □

COROLLARY 162. *There are $\phi(\phi(p)) \ge 1$ primitive roots mod p.*

5.3. Primitive roots mod p^2, p^k

Idea: linear deformation.

THEOREM 163. *Let r be a primitive root mod p. Then one of $r, r+p$ is a primitive root mod p^2.*

PROOF. By Euler's Theorem, $\mathrm{ord}_{p^2}(r)|\phi(p^2) = p(p-1)$. Also, $r^{\mathrm{ord}_{p^2}(r)} \equiv 1\,(p)$ so $p-1 = \mathrm{ord}_p(r)|\,\mathrm{ord}_{p^2}(r)$. If $\mathrm{ord}_{p^2}(r) < p(p-1)$ it must equal $p-1$.

Now consider $\mathrm{ord}_{p^2}(r+pt)$. Since $r+pt \equiv r\,(p)$ the same reasoning shows that $p-1|\,\mathrm{ord}_{p^2}(r+pt)|p(p-1)$. Moreover,

$$\begin{aligned}(r+pt)^{p-1} &= r^{p-1} + (p-1)r^{p-2}pt + \sum_{k=2}^{p-1}\binom{p-1}{k} r^{p-1-k}t^k p^k \\ &\equiv 1 - r^{p-2}tp\,(p^2)\,.\end{aligned}$$

Note that $p \nmid r^{p-2}$ so as long as $p \nmid t$ (say if $t=-1$) we have $p^2 \nmid (r+pt)^{p-1} - 1$ so $\mathrm{ord}_{p^2}(r+tp) \ne p-1$. □

THEOREM 164. *[not covered in class] Let p be odd and let r be a primitive root mod p^2. Then r is a primitive root mod p^k, $k \ge 2$.*

PROOF. Assume by induction that $\mathrm{ord}_{p^k} r = p^{k-1}(p-1)$. It follows that $r^{p^{k-2}(p-1)} \not\equiv 1\,(p^k)$. Since $r^{p^{k-2}(p-1)} \equiv 1\,(p^{k-1})$, we have $r^{p^{k-2}(p-1)} = 1 + tp^{k-1}$ for some t not divisible by p. It follows that

$$r^{p^{k-1}(p-1)} = (1+tp^{k-1})^p = 1 + tp^k + \sum_{l=2}^{p-1}\binom{p}{l} t^l p^{l(k-1)} + t^p p^{p(k-1)}\,.$$

Now if $k,l \ge 2$ then $l(k-1)+1 \ge 2(k-1) = k+1+(k-2) \ge k+1$ and $p \mid \binom{p}{l}$ if $2 \le l \le p-1$. Finally, if $p \ge 3$ then $p(k-1) \ge 3(k-1) = k+1+2(k-2) \ge k+1$ as well so

$$r^{p^{k-1}(p-1)} \equiv 1 + tp^k \not\equiv 1\,(p^{k+1})\,.$$

□

5.4. Discrete Log and ElGamal

See textbook.

CHAPTER 6

Quadratic reciprocity

6.1. Quadratic residues

Fix an odd prime p.

DEFINITION 165. Let a not be divisible by p. Call a a *quadratic residue* mod p if there is $x \in \mathbb{Z}$ such that $x^2 \equiv a\,(p)$. Otherwise say that x is a *quadratic non-residue*.

NOTATION 166. The *Legendre Symbol* is given by:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ a quadratic residue} \\ -1 & a \text{ a quadratic nonresidue} \\ 0 & p|a \end{cases}.$$

We first study $\left(\frac{a}{p}\right)$ as a function of a.

EXAMPLE 167. List all squares mod $3,5,7,11$ and obtain the residues and non-residues.

PROPOSITION 168. *(Euler's criterion)* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\,(p)$.

PROOF. If $p|a$ both sides vanish mod p. Otherwise, this is the case $n = 2$ of Theorem 157. □

EXAMPLE 169. For which primes amond $3,5,7,11$ is -1 a square mod p?

COROLLARY 170. *(The quadratic character of -1)* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1\,(4) \\ -1 & p \equiv 3\,(4) \end{cases}$.

REMARK 171. For an alternative proof see PS6.

LEMMA 172. *Let $a, a', b \in \mathbb{Z}$ with $a \equiv a'\,(p)$. Then:*

(1) $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$;
(2) $\left(\frac{b^2}{p}\right) = 1$ *if* $p \nmid b$;
(3) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

PROOF. The first two claims are true by definition ($x^2 \equiv a\,(p)$ iff $x^2 \equiv a'\,(p)$). For the third, it is clear if p divides one of a, b or if at least one is a quadratic residue, but the claim that if both a, b are non-residues then ab is a residue is non-trivial. In any case using Euler's criterion it is easy to check that

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

and if signs are congruent mod p they are equal since $p \nmid 2$. □

Another criterion:

PROPOSITION 173. *(Gauss's Lemma) Let $p \nmid a$. Then $\left(\frac{a}{p}\right) = (-1)^s$ where s is the number of t, $1 \leq t \leq \frac{p-1}{2}$ such that the least positive residue of at is greater than $\frac{p-1}{2}$.*

PROOF. We evalute the product $\prod_{t=1}^{\frac{p-1}{2}}(at) = a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$ in another way. For this divide the numbers $1 \leq x \leq p-1$ into pairs $\{x, p-x\}$ ($x \neq p-x$ since p is odd). If at, at' belong to the same pair then either they are equal (at which point $t \equiv t'(p)$) or opposite, at which point $at \equiv -at'(p)$ forces $t \equiv -t'(p)$. Since the range $1 \leq t \leq \frac{p-1}{2}$ does not contain t, t' such that $t \equiv -t'(p)$ and since there are exactly $\frac{p-1}{2}$ pairs it follows that $\prod_{t=1}^{\frac{p-1}{2}}(at) \equiv \prod_{1 \leq x \leq \frac{p-1}{2}}(\pm x)(p)$ where the sign is $+$ or $-$ according to whether $at \equiv x$ or $at \equiv -x$. By assumption we have s minus signs, so

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv (-1)^s \prod_{x=1}^{\frac{p-1}{2}} x \equiv (-1)^s \left(\frac{p-1}{2}\right)!.$$

The factor $\left(\frac{p-1}{2}\right)!$ is invertible mod p and we are done by Euler's criterion. □

COROLLARY 174. *(The quadratic character of 2)*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1\,(8) \\ -1 & p \equiv \pm 3\,(8) \end{cases}.$$

PROOF. Explicit count using Gauss's Lemma. □

6.2. Quadratic reciprocity

Now consider $\left(\frac{a}{p}\right)$ as a function of p. Euler observed that this only depends on the class of p mod $4a$. Gauss eventually proved this:

THEOREM 175. *(Gauss) Let p, q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & p \equiv q \equiv 3\,(4) \\ +1 & \textit{otherwise} \end{cases}.$$

PROOF. (Based on Exercize 17 to section 11.2) Let $R = \left\{1 \leq a \leq \frac{pq-1}{2} \mid (a, pq) = 1\right\}$, let $T = \left\{q, 2q, \cdots, \frac{p-1}{2}q\right\}$ and let $S = R \sqcup T = \left\{1 \leq a \leq \frac{pq-1}{2} \mid (a, p) = 1\right\}$ (if $(a, p) = 1$ then either $(a, pq) = 1$ or a is divisible by q). Finally, set $A = \prod_{a \in R} a$. One one hand we then have:

$$\begin{aligned} \prod_{a \in S} a &= \prod_{k=0}^{\frac{q-1}{2}-1} \prod_{j=1}^{p-1} (pk+j) \cdot \prod_{j=1}^{\frac{p-1}{2}} \left(p\frac{q+1}{2} + j\right) \\ &\equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!\,(p) \\ &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!\,(p) \end{aligned}$$

by Wilson's Theorem. On the other hand we have

$$\begin{aligned}\prod_{a\in S} a &= \left(\prod_{a\in R} a\right)\cdot\left(\prod_{j=1}^{\frac{p-1}{2}}(qj)\right)\\ &= Aq^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\\ &\equiv A\left(\frac{q}{p}\right)\left(\frac{p-1}{2}\right)!\,(p)\end{aligned}$$

by Euler's criterion (Proposition 168). Since $\left(\frac{p-1}{2}\right)!$ is invertible mod p and $\left(\frac{q}{p}\right)\equiv\pm 1\,(p)$ we conclude

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

By symmetry we also have

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

We now evaluate A mod pq. For this note that if x is a residue class mod pq then $x\not\equiv -x\,(pq)$ since p,q are odd. It follows that for each pair $\{x,-x\}$ of invertible residue class mod pq exactly one member belongs to A. Now let $a\in R$ and assume that $\bar{a}\not\equiv\pm a\,(pq)$. Then exactly one of $\bar{a},-\bar{a}$ belongs to R and together we get either a 1 or a -1 in A. Accordingly let $R'=\left\{1\le a\le\frac{pq-1}{2}\mid a^2\equiv\pm 1\,(pq)\right\}$. We have shown that:

$$A\equiv\pm\prod_{a\in R'} a\,(pq).$$

There are 4 residues a mod pq such that $a^2\equiv 1\,(p)$. Those are ± 1 and $\pm u$ where $u\equiv 1\,(p)$ and $u\equiv -1\,(q)$. There residues contribute $\pm u$ to A. Assume first that at least one of p,q is $\equiv 3\,(4)$. Then there is not x mod that prime such that $x^2\equiv -1$ mod that prime; a fortiori there is no a mod pq such that $a^2\equiv -1\,(pq)$ and hence $A\equiv\pm u\,(pq)$. It follows that $A \mod p$ and $A \mod q$ are opposite signs. If $p\equiv 1\,(4)$ and $q\equiv 3\,(4)$ this means that $-\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ have opposite signs (as claimed), while if $p\equiv q\equiv 3\,(4)$ it means that $-\left(\frac{p}{q}\right)$ and $-\left(\frac{q}{p}\right)$ have opposite signs (as claimed). We are left with the case $p\equiv q\equiv 1\,(4)$. Now fix ε,δ such that $\varepsilon^2\equiv -1\,(p)$ and $\delta^2\equiv -1\,(q)$. By the CRT there is v mod pq such that $v\equiv\varepsilon\,(p)$ and $v\equiv\varepsilon\,(q)$. Then the solutions to $a^2\equiv -1\,(pq)$ are $\pm v,\pm uv$, and R' contains precisely one from each pair, so that $A\equiv\pm u\cdot\pm v\,(\pm uv)\equiv\pm u^2\equiv\pm 1$. It follows that $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are congruent to the same sign mod pq, and hence they are equal. □

REMARK 176. Alternative proof: Let $G=\sum_{a(p)}\left(\frac{a}{p}\right)\zeta^a$ be the Gauss sum mod p. Then $\bar{G}=\sum_{a(p)}\left(\frac{a}{p}\right)\zeta^{-a}=\left(\frac{-1}{p}\right)G$ so $\left(\frac{-1}{p}\right)G^2=|G|^2=p$ by Planchere's formula. We thus have

$$p^{\frac{q-1}{2}}=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}G^{q-1}$$

and

$$\begin{aligned} Gp^{\frac{q-1}{2}} &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} G^q \\ &\equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \sum_{a(p)} \left(\frac{a}{p}\right)^q \zeta^{-aq}(q) \\ &\equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) G(q). \end{aligned}$$

Multiplying by G we find:

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

Since G^2 is invertible mod q we conclude

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

as a congruence in $\mathbb{Z}[\zeta]$. However, if a rational number is an algebraic integer then it is an integer, so this congruence holds in $\mathbb{Z}$ and both sides are equal.

ALGORITHM 177. *To evaluate* $\left(\frac{a}{p}\right)$*:*

(1) *Reduce a mod p to get a'.*
(2) *Factor a', and eliminate any square factors.*
(3) *For any prime factor q of a', relate* $\left(\frac{q}{p}\right)$ *to* $\left(\frac{p}{q}\right)$ *using QR, and evaluate the latter recursively.*

6.3. The Jacobi Symbol

Better algorithm: *avoid factoring*.

DEFINITION 178. Let P be an odd positive integer, with prime factorization $P = \prod_i p_i$ (the p_i need not be distinct). For $a \in \mathbb{Z}$ the *Jacobi symbol* is the function

$$\left(\frac{a}{P}\right) \stackrel{\text{def}}{=} \prod_i \left(\frac{a}{p_i}\right).$$

LEMMA 179. *Let $a, a', b \in \mathbb{Z}$ with $a \equiv a'(P)$. Then:*

(1) $\left(\frac{a}{P}\right) = \left(\frac{a'}{P}\right)$*;*
(2) $\left(\frac{b^2}{P}\right) = 1$ *if* $(P,b) = 1$*;*
(3) $\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$.

PROOF. These all follow from the respective properties of the Legendre symbol. □

THEOREM 180. *Let P, Q be odd nad positive. 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) $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$.

PROOF. In both (1),(2) the claim holds for P prime. Both sides of the claimed equality are also completely multiplicative (clear on the Jacobi Symbol side and an easy calculation on the other) so the claim follows). For part (3) one checks that both sides are separately completely multiplicative in P, Q (for the RHS this is already checked for part (1)) so again equality follows from the case of primes, which is the law of QR. □

ALGORITHM 181. *To evaluate* $\left(\frac{a}{P}\right)$*:*

(1) *Reduce a mod P to get* a'.

(2) *Write* $a' = 2^t Q$ *with Q odd. We then have* $\left(\frac{a}{P}\right) = \left(\frac{a'}{P}\right) = \left(\frac{2}{P}\right)^t \left(\frac{Q}{P}\right)$.

(3) *Evalute* $\left(\frac{2}{P}\right)$ *by part (2), and* $\left(\frac{Q}{P}\right)$ *by relating it to* $\left(\frac{P}{Q}\right)$ *and continuing recursively.*

CHAPTER 7

Special topics

7.1. The Gaussian integers

Baseically a review of the course but using a different number system.

- Defined the rings $\mathbb{Q}(i)$ and $\mathbb{Z}[i]$.
- State that they are rings.
- Define conugation and the norm; relate it to divisibility in $\mathbb{Q}(i)$.
- Find all units of $\mathbb{Z}[i]$.
- Divisition with remainder in $\mathbb{Z}[i]$ by rounding quotient in $\mathbb{Q}(i)$.
- Divisibility:
  - Only finitely many divisors;
  - define *gcd*;
  - Euclid's Lemma still holds. Due to division with remainder Euclid's Algorithm also still holds.
  - Bezout's extension also holds, and can also proof Bezout's Theorem by considering a minimal element of the ideal generated by z, w. This also shows the GCD is unique up to associates.
- Unique factorization
  - Define *irreducible*, *prime*. Discuss associates.
    - If $Nz = p$ is a rational prime then z must be irreducible.
  - Show that every Guassian integer is a product of irreducibles.
  - Show that π is prime iff it is irreducible and not a unique.
  - Conclude that the prime factorization is unique up to permutation and associates.
- Classification of primes.
  - If π is prime then π divides $N\pi$ which is a rational integer, and hence a product of rational primes. It follows that $\pi | p$ for some rational prime p.
  - If $N\pi = p^2 = Np$ then π is assoc to p. Otherwise $N\pi = p$.
  - $2 = -i(1+i)^2$ so $1+i$ is the only prime dividing 2.
  - If $p \equiv 3\,(4)$ and $p | a^2 + b^2$then $p|a, p|b$ (if $p \nmid a$ then $(\bar{a}b)^2 \equiv -1\,(p)$). It follows that p is not a norm, so p is still prime in $\mathbb{Z}[i]$.
  - If $p \equiv 1\,(4)$ then there is $a \in \mathbb{Z}$ such that $p \mid a^2 + 1$. But $p \nmid a \pm i$ in $\mathbb{Z}[i]$ so p is not prime. It follows that there is a prime properly dividing p so $N\pi = p$. This says $p = \pi\bar{\pi}$ and the two are not associates: $\frac{\pi}{\bar{\pi}} = \frac{\pi^2}{p} \notin \mathbb{Z}[i]$, so p is divisible by exactly two primes (and we can write $p = a^2 + b^2$ in 8 ways, coming from the 4 associates of $\pi, \bar{\pi}$ each).

7.2. Elliptic curves

$y^2 = x^3 + ax + b$.

- Plane cubics; the addition law.
- Fermat descent for $x^4 + y^4 = z^2$.
- Modularity
- Elliptic curves mod p.
- Elliptic curve cryptography.