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:
$$\left.\frac{rs}{(r,s)^2}\right| t \qquad \text{and} \qquad t \left| \frac{rs}{(r,s)}\right. .$$

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 $f \le e-1$ 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

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

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 $a^n \ne 1$ 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 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. Shwo that $b \in (\mathbb{Z}/m\mathbb{Z})^\times \setminus B'$ implies $bB' \cap B' = \emptyset$ and conclude that $|B| \le |B'| \le \frac{1}{2}\left|(\mathbb{Z}/m\mathbb{Z})^\times\right|$.

ALGORITHM. *(Rabin) Input: an integer $m \ge 2$.*

(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 $a \in \{1, \dots, m-1\}$, 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 "composite" 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 $1 \le a \le m-1$ efficiently calculate $a, a^2, a^4, a^8, a^{16}, \dots$ 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).