Math 445 Number Theory

Topics for the first exam

An integer $p$ is *prime* if whenever $p = ab$ with $a, b \in \mathbb{Z}$, either $a = \pm p$ or $b = \pm p$ .
[For sanity's sake, we will take the position that primes should also be $\geq 2$ .]

**Primality Tests.**

How do you decide if a number $n$ is prime?

Brute force: try to divide every number (better: prime) $\leq n$ (better $\leq \sqrt{n}$) into $n$, to locate a factor.

*Fermat's Little Theorem.* If $p$ is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 (\text{mod } p)$ .

A composite number $n$ for which $a^{n-1} \equiv 1 (\text{mod } n)$ is called a *pseudoprime to the base a.* A composite number which is a pseudoprime to every base $a$ satisfying $(a, n) = 1$ is called a *Carmichael number.*

$\phi(n)$ = number of integers $a$ between 1 and $n$ with $(a, n) = 1$; if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of $n$, then $\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)$

*Euler's Theorem.*If $(a, n) = 1$, then $a^{\phi(n)} (\text{mod } n)$ .

Fermat $\Rightarrow$ if $(a, n) = 1$ and $a^{n-1} \not\equiv 1 (\text{mod } n)$ then $n$ is **not** prime.

If $p$ is prime and $a^2 \equiv 1 (\text{mod } p)$, then $a \equiv \pm 1 (\text{mod } p)$

(Miller-Rabin Test.) Given $n$, set $n - 1 = 2^k d$ with $d$ odd. Then if $n$ is prime and $(a, n) = 1$, either $a^d \equiv 1 (\text{mod } n)$ or $a^{2^i d} \equiv -1 (\text{mod} n)$ for some $i < k$.

If $n$ is *not* prime, but the above still holds for some $a$, then $n$ is called a *strong pseudoprime to the base a.*

Compositeness test: If $a^d \not\equiv \pm 1 (\text{mod } n)$, compute $a^{2^i d} (mod n)$ for $i = 1, 2, \ldots$ . If this sequence hits 1 **before** hitting $-1$, or is not 1 for $i = k$, then $n$ is **not** prime.

Fact: If $n$ is composite, then it is a strong pseudoprime for *at most* $1/4$ th of the $a$'s between 1 and $n$.

**Finding Factors.**

(Pollard Rho Test.) Idea: if $p$ is a factor of $N$, then for any two randomly chosen numbers $a$ abd $b$, $p$ is more likely to divide $b - a$ than $N$ is.

Procedure: given $N$, use Miller-Rabin to make sure it is composite! Then pick a fairly random starting value $a_1 = a$, and a fairly random polynomial with integer coefficients $f(x)$ (such as $f(x) = x^2 + b$), then compute $a_2 = f(a_1), \ldots, a_n = f(a_{n-1}), \ldots$ . Finally, compute $(a_{2n} - a_n, N)$ for each $n$. If this is $> 1$ and $< N$, stop: you have found a proper factor of $N$. If it gives you $N$, stop: the test has failed. You should restart with a different $a$ and/or $f$.

Basic idea: this will typically find a factor on a timescale on the order of $\sqrt{p} \leq N^{1/4}$, where $p$ is the smallest (but unknown!) prime factor of $N$.

**RSA cryptosystem:**

To send and receive messages securely: start by choosing two large primes $p, q$ , set $n = pq$, and choose an $e$ relatively prime to $(p-1)(q-1)$ . Publish $n$ and $e$. Privately compute $d$ with $de - x(p-1)(q-1) = 1$ . To send you a message, we convert the message to a number $A$ (cutting it into blocks shorter than $n$ if necessary), compute $B = A^e \pmod{n}$ and send $B$. You then compute (because of Euler's Theorem!) $A = B^d \pmod{n}$ .

The security of the system rests on the fact that, to the best of our current knowledge, the fastest way to recover $A$ from $B$ is to determine $d$ (in order to do *your* calculations), which seems to require knowing $(p-1)(q-1)$, which amounts to knowing $p$ and $q$, which means factoring $n$, which is *hard*!

**Periods of repeating fractions.**

For integers $n$ with $(10, n) = 1$, the fractions $a/n$ have a repeating decimal expansion. E.g, $2/3 = .6666\ldots$, $1/7 = .142857142857\ldots$, etc.

Determining the length of the *period* (repeating part) can be done via FLT: $1/7 = .142857142857\ldots$ means $1/7 = 142857/10^6 + 142857/10^{12} + \ldots = 142857/(10^6 - 1)$, i.e $7|10^6 - 1$, and 6 is the smallest power for which this is true.

In general (if $(a, n) = 1$), we define $ord_n(a) = k$ = the smallest positive number with $a^k \equiv 1 \pmod{n}$. Equivalently, it is the largest number satisfying $a^r \equiv 1 \pmod{n} \Rightarrow ord_n(a)|r$ . (Therefore, $ord_n(a)|\phi(n)$, by Euler's Theorem.)

Generally, then, the period of $1/n = ord_n(10)$, when $(10, n) = 1$. When $(10, n) > 1$, we can write $n = 2^r 5^s b = ab$ with $(10, b) = 1$, and then write

$\frac{1}{n} = \frac{1}{ab} = \frac{A}{a} + \frac{B}{b}$ for some integers $A, B$ .

$A/a$ will have a terminating decimal expansion, so $1/n$ will have some garbage at the beginning , and then repeat with period equal to the period of $b$.

Gauss conjectured that there are infinitely many primes $p$ whose period is $p - 1$; this is still unproved.

**Primitive roots.**

A number $a$ is called a *primitive root of 1 mod* $n$ if $ord_n(a) = \phi(n)$ (the largest it could be).

If $n$ is prime, then there is a primitive root of 1 mod $n$.

The proof uses the important

(*Lagrange's Theorem.*) If $p$ is a prime, and $f(x) = a_n x^n + \cdots a_1 x + a_0$ is a polynomial with integer coefficients, $a_n \not\equiv 0 \pmod{p}$, then the equation

$$f(x) \equiv 0 \pmod{p}$$

has at most $n$ solutions.

This implies that if $p$ is prime and $d|p-1$, then the equation $x^d \equiv 1 \pmod{p}$ has *exactly* $d$ solutions.

Finding a primitive root mod $p$ a prime: for each prime $p_i|p-1$, find $a_i$ with $a_i^{(p-1)/p_i} \not\equiv 1 \pmod{p}$, then set $a$ = the product of the $a_i$.

Lemma: If $ord_n(a) = m$, then $ord_n(a^k) = m/(m, k)$

Corollary: If $p$ is prime, then there are exactly $\phi(p-1)$ (incongruent mod $p$) primitive roots of 1 mod $p$: find one, $a$, then the rest are $a^k$ for $1 \le k \le p$ and $(k, p-1) = 1$.

A faster factoring algorithm: **the quadratic sieve.**

Originates with Fermat: for $n$ odd, if composite then $n = a^2 - b^2 = (a+b)(a-b)$ for some $a, b$. Finding such a factorization is slower than trial division!

Improvement: find $a_i$ close to $\sqrt{n}$ so that $a_i^2 - n = b_i$ have product a square: $b_1 \cdots b_k = x^2$, so $n | (a_1 \cdots a_k)^2 - x^2$, and $(n, a_1 \cdots a_k + x)$ or $(n, a_1 \cdots a_k - x)$ might produce a proper factor.

Finding the $a_i$: choose a bound $B$ and search for $b_i$ whose prime factors are all $\leq B$ ($B$-smooth numbers). If there are $m$ primes $\leq B$, then with $m+1$ such $b_i$ some product of them must be a square. The right collection can be found by linear algebra: create vectors listing the exponents of the primes in the factorization of $b_i$, mod 2, and find a collection which sum to the 0-vector, mod 2.

Finding the $b_i$; start with $a = \lfloor \sqrt{n} \rfloor + 1$ and $(a+i)^2 - n = b_i$; for a prime $p \leq B$, $p | b_i$ if $(a+i)^2 \equiv n \pmod{p}$; this is true either never (if $x^2 \equiv n$ has no solutions) or for two values $n_1, n_2$ mod $p$ (see below!). Only $a + i = n_k + jp$ can yield a $b_i$ that is a multiple of $p$; finding such $b_i$ that are divisble by many $p$ yields $B$-smooth numbers.

**Pythagorian triples:**

If $a^2 + b^2 = c^2$, then we call $(a, b, c)$ a Pythagorean triple. If $(a, b) = 1$ then $((a, c) = (b, c) = 1$ and) we call the triple *primitive*. For a primitive triple, $c$ must be odd, $a$ (say) even and $b$ odd. Then because

*Proposition:* If $(x, y) = 1$ and $xy = c^2$, then $x = u^2, y = v^2$ for some integers $u, v$ .

we can write $a = 2uv$ , $b = u^2 - v^2$ , and $c = u^2 + v^2$ for some integers $u, v$ ; these formulas describe *all* primitive Pythagorean triples.

**Sums of squares.**

If $n = a^2 + b^2$, then $n \equiv 0, 1,$ or $2 \pmod{4}$. Since the product of the sum of two squares
$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$
is the sum of two squares, and
$2n = (a^2 + b^2) \Rightarrow n = (\frac{a-b}{2})^2 + (\frac{a+b}{2})^2$ and $m = (a^2 + b^2) \Rightarrow 2m = (a-b)^2 + (a+b)^2$
it suffices to focus on odd numbers, and (more or less) odd primes.

If $p \equiv 1 \pmod{4}$ is prime, then $p$ is the sum of two squares.

If $p \equiv 3 \pmod{4}$ is prime and $p | a^2 + b^2$, then $p | a$ and $p | b$.

Together, these imply that a positive integer $n$ can be expressed as the sum of two squares $\Leftrightarrow$ in the prime factorization of $n$, every prime congruent to 3 mod 4 appears with even (possibly 0) exponent.

**$n^{th}$ roots modulo a prime:**

If $p$ is prime and $(a, p) = 1$, then (setting $r = (n, p-1)$ the equation $x^n \equiv a \pmod{p}$ has

$r$ solutions if $a^{(p-1)/r} \equiv 1 \pmod{p}$

no solution if $a^{(p-1)/r} \not\equiv 1 \pmod{p}$

(Euler's Criterion.) The equation $x^2 \equiv a \pmod{p}$ has a solution ($p =$ odd prime) $\Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$ ; it then has two solutions ($x$ and $-x$).

The equation $x^2 \equiv -1 \pmod{p}$ has a solution $\Leftrightarrow (-1)^{(p-1)/2} \equiv 1 \pmod{p} \Leftrightarrow p = 2$ or $p \equiv 1 \pmod{4}$

**Solving $x^2 \equiv a \pmod p$: the algorithm RESSOL.**

If it has a solution, then $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ . Let $p-1 = 2^k m$ with $m$ odd, and set $r \equiv a^{\frac{m+1}{2}} \pmod p$, and $n \equiv a^m$. Then $r^2 \equiv a^{m+1} = a \cdot n$, and $n^{2^{k-1}} \equiv a^{\frac{p-1}{2}} \equiv 1$, so $\mathrm{ord}_p(n) = 2^{k_1}$ for some $k_1 < k$. The goal: by altering $r$, whittle $n$ down to 1.

We also need a quadratic <u>non</u>-residue, i.e., a $b$ with $b^{\frac{p-1}{2}} \equiv -1 \pmod p$. (Find one by computing $b^{\frac{p-1}{2}}$ for random $b$; half of all guesses will be non-residues.) Then setting $c = b^m$, $\mathrm{ord}_p(c) = 2^k$, so $\mathrm{ord}_p(c^{2^{k-k_1}}) = 2^{k_1}$. Then we use:

If $\mathrm{ord}_p(x) = \mathrm{ord}_p(y) = 2^r$, then $\mathrm{ord}_p(xy) = 2^s$ with $s < r$.

Then setting $r_1 = c^{2^{k-k_1-1}}$, $(rr_1)^2 \equiv a(c^{2^{k-k_1}}n) = an_1$, with $\mathrm{ord}_p(n_1) = 2^{k_2}$ for $k_2 < k_1$. Now do it again! Continuing this process will yield $x = rr_1 \cdots r_k$ with $(rr_1 \cdots r_k)^2 \equiv an_k$ and $\mathrm{ord}_p(n_k) = 2^0 = 1$, i.e., $n_k = 1$, giving $x^2 \equiv a$.

Note that we need to know the precise order of $n_i$ at each step (which power of 2), which can be found by repeated squaring.