1 Fri 10.23

Miller-Rabin Test

Let N be an odd integer. We write $N - 1 = 2^k \cdot q$ with q odd. If there exists an integer $a < n$ such that

(1) $a^q \not\equiv 1 \pmod{N}$ and

(2) $a^q, a^{2q}, a^{4a}, \ldots, a^{2^{k-1}q} \not\equiv -1 \pmod{N}$

then we conclude that N is a composite number and say a is a *strong witness*. One strong witness of such a suffices to show N is composite, **but no conclusion can be drawn on whether N is prime if one of the two conditions fail for one a.**

Example 1.1

Let $N = 9$ and so $9 - 1 = 2^3 \cdot 1 = 2^k \cdot q$.

A useless test: let $a = 1$. Then we have

$$a^1 \equiv 1 \pmod{9} \implies \text{test fails, no conclusion can be drawn.}$$

A useful test: let $a = 2$. Then

$$\begin{cases} a^1 = 2 \not\equiv 1 \pmod{9} & \implies \text{condition (1) is met.} \\ \left.\begin{cases} 2^{1\cdot 1} \equiv 1 \pmod{9} \\ 2^{2\cdot 1} \equiv 4 \pmod{9} \\ 2^{4\cdot 1} \equiv 7 \pmod{9} \end{cases}\right\} & \implies \text{condition (2) is met.} \end{cases}$$

From above we see that $a = 2$ is a strong witness and hence 9 is a composite.

Theorem 2

Let $N > 1$ be odd and composite. The probability that an integer between 2 and $N - 2$ is a Miller-Rabin test witness is greater than 75%. This gives rise to the fact that, if we pick t numbers, all of which fail to be strong witnesses, then the probability that N is composite is less than 4^{-t}.

Proposition 3

A easier version: at least 50% among $\{1, 2, \ldots, N-1\}$ are strong witnesses if N is odd and composite. Let $N - 1 = 2^b \cdot q$.

Proof

We say a is not a strong witness if

$$a^q \equiv 1 \pmod{N}$$

or

$$a^{2^i q} \equiv -1 \pmod{N}$$

for some $0 \leqslant i \leqslant b-1$.

First thing to notice: if a raised to some power is 1 or -1 mod N, we know that $\gcd(a, N) = 1$ because otherwise we would have a immediate contradiction over the divisibility of the gcd. Therefore
a not being a strong witness $\implies a \in (\mathbb{Z}/N\mathbb{Z})^*$.

Now we want to find a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ that contains *all* strong witnesses — if this group can be found, then by Lagrange's theorem this group can be of order at most $\varphi(n)/2 \leqslant (N-1)/2$.

The construction of such subgroup consists of two scenarios:

(1) If $N = p^\alpha$, i.e., a prime power. Clearly p is an odd prime. Recall that $N - 1 = p^\alpha - 1 = 2^b \cdot q$. On one hand, Euler's theorem states that

$$a^{\varphi(N)} \equiv a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{N} \tag{1}$$

while on the other hand, since a is not a strong witness, either $a^q \equiv 1$ or

$$a^{2^j q} \equiv -1 \pmod{N} \text{ for some } 0 \leqslant j \leqslant b-1.$$

In the first case, $a^q \equiv 1$ implies $a^{2^b q} = (a^q)^{2^b} \equiv 1 \pmod{N}$, and in the second case squaring both sides gives $a^{2^{j+1} q} \equiv (-1)^2 \equiv 1 \pmod{N}$ and, again, $a^{2^b q} = (a^{2^{j+1} q})^* = 1^* \equiv 1 \pmod{N}$ with $* = 2^{b-j-1}$. In either case, we know

$$a^{2^b q} \equiv 1 \pmod{N}. \tag{2}$$

Then, using (1) and (2), we see that, if $o(a) = x$, then $x \mid \gcd(2^b q, \varphi(N)) = \gcd(p^\alpha - 1, p^{\alpha-1}(p-1))$.

□

2 Mon 10/26

Continuing the proof of last class:

Proof

(1) Since $\gcd(p^\alpha - 1, p^{\alpha-1}(p-1)) = p-1$, we've shown that if a is a nonwitness, $a^{p-1} \equiv 1 \pmod N$. Now we just need to show that $\{a \mid \gcd(a, N) = 1 \text{ and } a^{p-1} \equiv 1 \pmod N\}$ is a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Recall that if $N = p^\alpha$ then

$$(\mathbb{Z}/N\mathbb{Z})^* = \{1, 2, \ldots, p-1, p+1, \ldots, 2p-1, 2p+1, \ldots\}.$$

Suppose it's not a proper subgroup, i.e., the groups are "equally large". Let $b = p+1$, then

$$(p+1)^{p^\alpha} \equiv 1 \pmod{p^\alpha} \text{ (by binomial expansion)}$$

This means if $p+1$ has order x in $(\mathbb{Z}/N\mathbb{Z})^*$ then $x \mid p^\alpha$, but any divisor of p^α (besides the trivial 1) will not divide $p-1$ and so this is a contradiction, i.e., we've found something in $(\mathbb{Z}/N\mathbb{Z})^*$ but not the "equally large subgroup". Hence our group needs to be a proper subgroup. Then its size is at most half of that of $(\mathbb{Z}/N\mathbb{Z})^*$ which is $\varphi(N) \leqslant N-1$. Thus there's at most $< 50\%$ nonwitness in this case.

(2) The other case is omitted. Refer to handout.

□

Suppose $x^2 \equiv y^2 \pmod n$. Then $n \mid (x+y)(x-y)$. There is a decent chance that either $\gcd(N, x-y), \gcd(N, x+y)$ is nontrivial. See **method of squares.**

Example 2.1

Suppose we know $188^2 \equiv 2^2 \pmod{589}$, then $589 \mid (188-2)(188+2) = 186 \cdot 190$. In fact $589 = 31 \cdot 19$, $186 = 31 \cdot 6$, and $190 = 19 \cdot 10$.

Proposition 4

How does one come up with $x^2 \equiv y^2 \pmod n$?

(1) Heuristics / methods to come up with a lot of numbers $a_1, a_2, \ldots$ such that

$$a_i^2 \equiv c_i \pmod n$$

where c_i factors as a product of small primes.

Example 2.2

Let $N = 914387$. Then $a_1^2 \equiv 1068^2 \equiv 750000 \equiv 2^4 \cdot 3 \cdot 5^6 \pmod{N}$.

3 Wed 10/28

A more efficient algorithm when computing $2^{50} \pmod{27}$: we get $2^2, 2^4, 2^8, 2^{16}, 2^{32}$, and $2^{50} = 2^{32+16+2}$. Here we reduce the number steps required fro 2^n from n to $2 \ln n$.

4 Mon 11/2

From last time [I took no notes] we have the following:

Proposition 5

Suppose $N = pq$ a product of two distinct primes, then $\varphi(N) = (p-1)(n-1)$. Suppose we want to solve

$$x^e \equiv c \pmod{N} \text{ where } \gcd(c, N) = 1$$

and further suppose $\gcd(e, \varphi(N)) = 1$, then $x \equiv c^d \pmod{N}$ where d is any number satisfying $cd \equiv 1 \pmod{\varphi(N)}$.

5 Wed 11/4 Primitive Roots mod n

Assume $N \geqslant 2$. Recall that

$$G := (\mathbb{Z}/n\mathbb{Z})^* = \{a \mid \gcd(a, n) = 1 \text{ and } a \in [1, n]\}.$$

We know G is a group under multiplication mod n and $|G| = \varphi(n)$. Euler's theorem states that $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Definition 6

Pick $a \in G$. It is called a **primitive root** mod n if $o(a) = \varphi(n)$ in G. Equivalently, $a \in G$ is called a primitive root mod n if it's a generator of $(\mathbb{Z}/n\mathbb{Z})^*$.

Example 5.1

Consider $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$. Hence $\varphi(12) = 4$. Here $o(1) = 1, o(11) = o(5) = o(7) = 2$. This implies there are no primitive roots mod 12.

Remark

If we know there's at least one primitive root mod p, how many will there be?

In $(\mathbb{Z}/7\mathbb{Z})^*$, the orders of $1, 2, 3, 4, 5, 6$ are $1, 3, 6, 3, 6, 2$, respectively.

The answer: $\varphi(p-1)$. Proof: $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/p-1\mathbb{Z}$, see HW3 p3 / HW4 p1.

6 Fri 11/6

Suppose p is a prime and $(\mathbb{Z}/p\mathbb{Z})^*$ has a generator, then from the last lecture the total number of generators is $\varphi(p-1) = \varphi(\varphi(p))$. Generalization:

Theorem 7

Suppose n has a primitive root. Then the total number of primitive roots mod n is $\varphi(\varphi(n))$.

Proof

Let a be a primitive root mod n. Then

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a^0, a^1, a^2, \ldots, a^{\phi(n)}\} \text{ and so } |(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n).$$

For a^i to be a generator, it has to satisfy the requirement that $ki \equiv m \pmod{\varphi(n)}$ always has a solution. This gives rise to the fact that $\gcd(i, \varphi(n)) = 1$ (this is an iff statement), and thus there are $\varphi(\varphi(n))$ such i's. These are precisely $\varphi(\varphi(n))$ generators / primitive roots mod n. □

Problems to think about:

(1) How many distinct solutions mod p are there for the equation $x^{p-1} - 1 \equiv 0 \pmod{p}$, given p is a prime?

(2) How many distinct solutions mod p for $x^d - 1 \equiv 0 \pmod{p}$? Two cases: $d \mid p-1$ and $d \nmid p-1$.

(3) Given $n \geqslant 5$, which elements of $(\mathbb{Z}/n\mathbb{Z})^*$ are **not** going to be primitive roots? [Hint: $1, n-1$ will always be discarded. In addition, any a of form $a \equiv x^2 \pmod{n}$ will be discarded: let b be a primitive root and $a = x^2$.

Then $a = b^{2i}$ and a can only generate even powers of p. The order of a is $\varphi(n)/\gcd(2i, \varphi(n))$. But $\varphi(n)$ is always even (for large n).]

Artin Conjecture

There exist infinitely many primes p such that

$$a \not\equiv 1, -1, x^2 \pmod p \implies a \text{ is a primitive root.}$$

7 Mon 11/9

Theorem 9

If $n = 2^k$ for $k \geqslant 3$, then it has no primitive roots mod n.

Proof

Notice that

$$\varphi(n) = 2^{k-1}$$

which means if a with $\gcd(a, n) = 1$ is a primitive root mod n we get $o(a) = 2^{k-1}$. Then by definition $a^{\varphi(n)} \equiv 1 \pmod n$ and so $o(a) \mid 2^{k-1}$. Positive orders of a are

$$2^0, 2^1, \dots, 2^{k-2}, 2^{k-1}.$$

By induction, for odd a we have $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ for $k \geqslant 3$. This gives the contradiction of a being a primitive root since no $a \in G$ has $o(a) = 2^{k-1}$. □

Theorem 10

Let $n = st$ where s, t are coprime and $\geqslant 3$. Then there's no primitive root mod n.

Proof

Since $\varphi(n) = \varphi(s)\varphi(t)$, any primitive root a with $\gcd(a, n) = 1$ satisfies $o(a) = \varphi(n) = \varphi(s)\varphi(t)$. Since $\gcd(a, n) = 1$ we know $\gcd(a, s) = \gcd(a, t) = 1$. By Euler we have

$$a^{\varphi(s)} \equiv 1 \pmod{s} \text{ and } a^{\varphi(t)} \equiv 1 \pmod{t}.$$

Let $\ell = \operatorname{lcm}(\varphi(s), \varphi(t)) = \varphi(s)\varphi(t)/\gcd(\varphi(s), \varphi(t))$. Then we have

$$a^{\ell} \equiv 1 \pmod{s} \text{ and } a^{\ell} \equiv 1 \pmod{t}$$

from which it follows that $st \mid a^{\ell} - 1$ since s, t are coprime. Then $a^{l} \equiv 1 \pmod{st} \;/\; \pmod{n}$. On the other hand, the assumption that $s, t \geqslant 3$ ensures that $\varphi(s), \varphi(t)$ are both even. Hence $\ell \leqslant \varphi(n)/2$ and we've derived a contradiction showing that a cannot be a primitive root. □

Remark

If n has two distinct odd prime factors then there is no primitive root mod n. Obvious from above. Same thing if $n = 2^k p \cdot ()$ with $k \geqslant 2$.

Theorem 11

Let p be an odd prime and $k \geqslant 1$. Then $n = p^k$ and $m = 2p^k$ have primitive roots.

Proof

We will need this lemma first:

Lemma 7.1

If p is an odd prime, then we can find a primitive root r mod p with $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Proof. Pick r, a primitive root mod p. If $r^{p-1} \not\equiv 1 \pmod{p^2}$ then we are done.

Otherwise, notice that $\tilde{r} := r + p$ is still a primitive root mod p and

$$\begin{aligned}\tilde{r}^{p-1} &\equiv (r+p)^{p-1} \pmod{p^2}\\ &\equiv r^{p-1} + (p-1)r^{p-2}p + p^2[\dots] && \text{(binomial expansion)}\\ &\equiv r^{p-1} + (p-1)r^{p-2}p \pmod{p^2}.\end{aligned}$$

Clearly $p^2 \nmid (p-1)r^{p-2}p$ or otherwise $p \mid (p-1)r^{p-2} \implies p \mid r^{p-2}$, impossible since r is of order $\varphi(p) = p-1$. Therefore

$$\tilde{r}^{p-1} \not\equiv 1 \pmod{p^2}$$

and we are done. □

We now show that p^2 has a primitive root. Why? By the lemma there exists r, a primitive root mod p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$. By Euler, $a^{\varphi(p^2)} \equiv 1 \pmod{p^2}$ for any a with $\gcd(a, p^2) = 1 \iff \gcd(a, p) = 1$. Therefore

$$r^{p(p-1)} \equiv 1 \pmod{p^2}$$

which implies $o(r) \mid p(p-1)$ [with respect to $(\mathbb{Z}/p^2\mathbb{Z})^*$]. By lemma $o(r) \neq p-1$ and of course $r \neq 1$. Also $o(r) \neq p$ or $r^p = 1$, contradicting $r^{p-1} = 1$ (Fermat). Thus $o(r) = \varphi(p^2)$ and r is a primitive root. [to be continued...] □

8 Wed 11/11

Continuing the proof from last time:

Proof

Now we need to generalize the cases p and of p^2 to p^k.

Lemma 8.1

If p is an odd prime, then by the previous lemma there exists r, a primitive root, such that $r^{p-1} \not\equiv 1 \pmod{p^2}$. This can be generalized (by induction) to the following:

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Proof

Base case: $k = 2$ trivial.

Induction hypothesis: assume case k holds. We want to show

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

Suppose by contradiction that the above is actually $\equiv$. Then the following would also hold true:

$$r^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}.$$

Then, by Euler, in $(\mathbb{Z}/p^k\mathbb{Z})^*$,

$$\begin{cases} o(r) \mid p^{k-1}(p-1) \\ o(r) \nmid p^{k-2}(p-1) \end{cases} \implies o(r) = p^{k-1}(p-1).$$

Thus

$$\begin{cases} r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \\ r^{p^{k-1}(p-1)} = \left(r^{p^{k-2}(p-1)}\right)^p \equiv 1 \pmod{p^k} \end{cases}$$

Whereas in $(\mathbb{Z}/p^{k-1}\mathbb{Z})^*$ we have

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}} \implies p^{k-1} \mid r^{p^{k-2}(p-1)} - 1$$

so $r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$ for some $a \nmid p$ (otherwise $r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$ which we said no).

Applying binomial again:

$$\begin{aligned} r^{p^{k-1}(p-1)} &= \left(1 + ap^{k-1}\right)^p \\ &= 1 + p \cdot ap^{k-1} + \dots \\ &\equiv 1 + ap^k \pmod{p^{k+1}} \not\equiv 1 \end{aligned}$$

since ap^k cannot be 0 mod p^{k+1} given $a \nmid p$. This completes the proof of lemma by contradiction, and indeed $k \implies k + 1$. □

Suppose r is a primitive root satisfying the conditions above. Let the order of r in $(\mathbb{Z}/p^k\mathbb{Z})^*$ is n. Then $r^n \equiv 1 \pmod{p^k}$. Since

$$\varphi(p^k) = p^{k-1}(p-1)$$

by Euler's theorem we have

$$a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k} \text{ for all } a \text{ such that } \gcd(a, p^k) = 1.$$

Now we've got

$$\begin{cases} r^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k} \implies n \mid p^{k-1}(p-1) \\ r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \implies n \nmid p^{k-2}(p-1) \end{cases}$$

Along with the fact that r is a primitive root mod $p \implies n \mid p-1$ we see that the only possibility is $n = p^{k-1}(p-1) = \varphi(p^k)$, i.e., r is a primitive root mod p^k. □

9 Fri 11/13 Quadratic Reciprocity

Given integer a and prime p, we can determine whether a is a square mod p.

(1) $p = 2$ and a odd, then $x^2 \equiv a \pmod 2$ always has 1 as a solution. If a is even then $x^2 \equiv 2 \pmod 2$ always has 0 as a solution. *Every integer is a square mod* 2.

(2) $p = 3$. WLOG we can assume $a \in \{0, 1, 2\}$. $x^2 \equiv 0$ and 1 mod 3 have solutions but $x^2 \equiv 2 \pmod 3$ has no solution as $0^2, 1^2, 2^2$ all evaluate to something else. 2 *is not a square mod* 3.

(3) $p = 5$. Squaring $\{0, 1, 2, 3, 4\}$ gives $\{0, 1, 4, 9, 16\} = \{0, 1, 4, 4, 1\}$. *Hence* 2 *and* 3 *are not squares mod* 5.

(4) $p = 7$. Squaring $\{0, 1, 2, 3, 4, 5, 6\}$ gives $\{0, 1, 4, 9, 16, 25, 36\} = \{0, 1, 4, 2, 2, 4, 1\}$. *Hence* 3, 5, 6 *are not squares mod* 7.

Forget about 0. Now pick a. We have $(p-a)^2 = p^2 - 2pa + a^2 = a^2$ and so $a^2 \equiv (p-a)^2 \pmod p$ which explains why the sets above show some kind of symmetry when disregarding the first 0. Therefore all squares mod p have to come from the set

$$\{0^2, 1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}.$$

Furthermore, these elements are distinct. Otherwise, suppose $0 \leqslant i < j \leqslant (p-1)/2$ and $i^2 \equiv j^2 \pmod p$ which implies $p \mid (j+i)(j-i)$ which is clearly impossible. Therefore:

Theorem 12

Let p be an odd prime. The number of squares mod p is $(p+1)/2$.

Again, let p be an odd prime. There is a primitive root r mod p. Then

$$\{0,1,\dots,p-1\} = \{0\} \cup (\mathbb{Z}/p\mathbb{Z})^* = \{0, r^1, \dots, r^{p-1}\}.$$

Since 0 is clearly a square, the question becomes: for which i is $x^2 \equiv r^i \pmod p$ solvable? If r is even then $(r^{r/2})^2 \equiv r^i \pmod p$, done. Now suppose i is odd and is therefore of form $2k+1$. If it does have a solution then the solution must be of form r^j. Then

$$r^{2j} = r^{2k+1} \implies r^{2j-2k+1} \equiv 1 \pmod p.$$

On the other hand, by Fermat we have $o(r) = p-1$, even. Therefore $r^{\text{odd}} \equiv 1 \pmod p$ is clearly impossible.

Theorem 13

Let p be an odd prime and r a primitive root mod p. Then r^i is a square mod p if and only if i is even.

Remark

$$(\mathbb{Z}/p\mathbb{Z})^* = \underbrace{\{r^0, r^2, \dots, r^{p-3}\}}_{\text{squares}} \sqcup \underbrace{\{r^1, r^3, \dots, r^{p-2}\}}_{\text{non-squaures}} \quad (\text{note that } r^0 = r^{p-1}).$$

Now we have:

(1) square times square is square

(2) square times non-square is non-square

(3) non-square times non-square is square [again!].

Definition 14

Given a an integer and p an odd prime, the **Legendre symbol** is defined as following:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is a non-square mod } p. \end{cases}$$

A key property that follows:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Euler's Criterion

Let p be an odd prime. If $\gcd(a,p) = 1$ then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Quadratic Reciprocity

Let p, q be odd primes. Then

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