



Number Theory

Book 3

Theorem Let p be an odd prime. Then

$$x^p - x = x(x^{p-1} - 1) = x \underbrace{(x^{\frac{p-1}{2}} - 1)}_{\text{Roots: all (nonzero) squares in } \mathbb{F}_p} \underbrace{(x^{\frac{p-1}{2}} + 1)}_{\text{Roots: all nonsquares in } \mathbb{F}_p} = x(x-1)(x-2)\dots(x-(p-1))$$

Every $a \in \mathbb{F}_p$ is a root of $x^p - x$.
(Fermat's Little Theorem)

Proof Let $a \in \mathbb{F}_p$, $a \neq 0$, so a^2 is a nonzero square in \mathbb{F}_p . Then a^2 is a root of $x^{\frac{p-1}{2}} - 1$ since $(a^2)^{\frac{p-1}{2}} - 1 = a^{p-1} - 1 = 0$ by Fermat's Little Theorem.
So by process of elimination, $x^{\frac{p-1}{2}} + 1$ has as its $\frac{p-1}{2}$ roots all the nonsquares in \mathbb{F}_p .

This gives a criterion for checking when an element $a \in \mathbb{F}_p$ is a square or a nonsquare. called Euler's Criterion: given $a \in \mathbb{F}_p$, p an odd prime,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{if } a \text{ is square nonzero} \\ -1 & \text{if } a \text{ is nonsquare} \\ 0 & \text{if } a = 0. \end{cases} \pmod{p}.$$

Eg. is 7 a square or a nonsquare in \mathbb{F}_{13} ? Use Euler's Criterion: $7^6 \equiv 10^3 \equiv 1000 \equiv 12 \equiv -1 \pmod{13}$.
So 7 is a nonsquare mod 13.

Definition Let p be an odd prime, $a \in \mathbb{Z}$. Then the Legendre symbol $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$

is defined by $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is nonzero square mod } p; \\ -1 & \text{if } a \text{ is nonsquare mod } p; \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$

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

eg. $\left(\frac{7}{13}\right) = -1$ $\left(\frac{0}{13}\right) = 0$
 $\left(\frac{10}{13}\right) = 1$ $\left(\frac{39}{13}\right) = 0$ $\left(\frac{20}{13}\right) = -1$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{for all } a, b \in \mathbb{Z} \quad (\text{they don't need to be relatively prime})$$

The Legendre symbol $\left(\frac{a}{p}\right)$ is a completely multiplicative function of a (where the odd prime p is fixed)

eg. $\underbrace{\left(\frac{20}{13}\right)}_{-1} = \underbrace{\left(\frac{4}{13}\right)}_{+1} \underbrace{\left(\frac{5}{13}\right)}_{-1} = -1$ so $20 \equiv 7 \pmod{13}$ is a nonsquare mod 13.

When is $-1 \equiv \square \pmod{p}$ a square mod p ? -1 is a $\begin{cases} \text{nonsquare mod } 3, 7, 11, \dots, 2003, \dots \\ \text{square mod } 5, 13 \end{cases}$

Is -1 a square or a nonsquare mod $p = 2003$? Nonsquare.

Theorem Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$

The quick proof uses $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

If $p = 4k+1$ then $\frac{p-1}{2} = 2k$, $(-1)^{2k} = 1$.

If $p = 4k+3$ then $\frac{p-1}{2} = 2k+1$, $(-1)^{2k+1} = -1$.

How hard is it to find a nonsquare mod p (given an odd prime p)?

Given $a \in \mathbb{Z}$, p odd prime, compute the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ nonzero square mod } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \\ -1 & \text{if } a \text{ nonsquare mod } p \end{cases}$$

We can use Euler's Criterion $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Easy on a computer; not so easy by hand.
 But there is a method that works well by hand: the method of Quadratic Reciprocity (Ch. 22).

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

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

eg. $\left(\frac{2}{7}\right) = 1$ since $2 \equiv 3^2 \pmod{7}$
 $7 \equiv -1 \pmod{8}$ so ...

$\left(\frac{2}{5}\right) = -1$ 1,4 squares mod 5
 2,3 nonsquares ...

If $p \neq q$ odd primes then $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are closely related:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{if at least one of } p, q \text{ is } \equiv 1 \pmod{4}$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{if } p \equiv q \equiv 3 \pmod{4}$$

i.e. $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ (the law of Quadratic Reciprocity)

Eg. Compute $\left(\frac{14}{47}\right) = \underbrace{\left(\frac{2}{47}\right)}_{+1} \left(\frac{7}{47}\right) = \left(\frac{7}{47}\right) = -\left(\frac{47}{7}\right) = -\left(\frac{5}{7}\right) = -(-1) = 1$ i.e. 14 is a square mod 47.

Since $47 \equiv -1 \pmod{8}$ Since $7 \equiv 3 \pmod{4}$

Eg. $\left(\frac{60}{89}\right) = \left(\frac{2^2 \cdot 3 \cdot 5}{89}\right) = \underbrace{\left(\frac{2}{89}\right)}_{+1} \left(\frac{3}{89}\right) \left(\frac{5}{89}\right) = \left(\frac{3}{89}\right) \left(\frac{5}{89}\right) = \left(\frac{89}{3}\right) \left(\frac{89}{5}\right) = (-1) \left(\frac{4}{5}\right) = (-1)(+1) = -1$ i.e. 60 is a nonsquare mod 89.

$89 \equiv 1 \pmod{4}$

Questions: If we compute $\left(\frac{a}{p}\right) = 1$ (either by Euler's Criterion or Quadratic Reciprocity) we know $x^2 \equiv a \pmod{p}$ has two solutions (the two square roots of $a \pmod{p}$). Can we actually find these two solutions? (i.e. compute the square roots of $a \pmod{p}$)? Yes.

eg. $p \equiv 1 \pmod{4}$, $\left(\frac{-1}{p}\right) = +1$. In this case we can find the two square roots of $-1 \pmod{p}$ rather easily even if p is thousands of digits long. As follows:

Pick $c \in \{1, 2, \dots, p-1\}$ randomly. Compute $\left(\frac{c}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ mod p .

If $\left(\frac{c}{p}\right) = -1$ (c is ~~not~~ square mod p) take $x \equiv c^{\frac{p-1}{4}}$ mod p , then $x^2 \equiv c^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

If $\left(\frac{c}{p}\right) = +1$ (c square mod p) try again.

99.9% of the time, it takes at most ten tries to find x satisfying $x^2 \equiv -1 \pmod{p}$.

How can we find $a, b \in \mathbb{Z}$ satisfying $p = a^2 + b^2$? (assuming $p \equiv 1 \pmod{4}$)

This is as difficult as finding a solution of $x^2 \equiv -1 \pmod{p}$.

If $p = a^2 + b^2$ then in \mathbb{F}_p , $a^2 + b^2 = 0$, $b^2 = -a^2$, $-1 = \left(\frac{a}{b}\right)^2$. The square roots of $-1 \pmod{p}$ are $\pm \frac{a}{b}$.