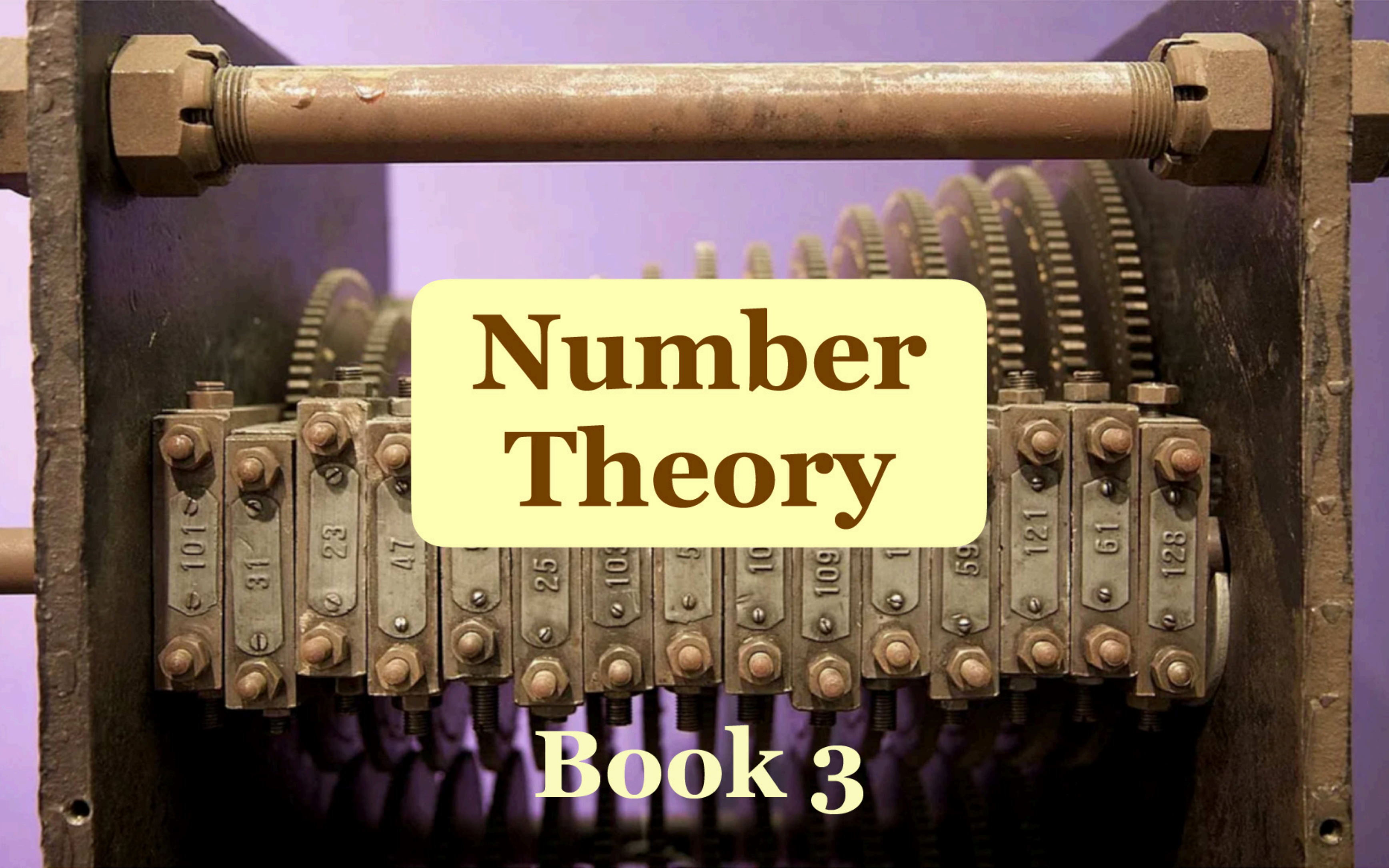

Number Theory

Book 3

Theorem Let p be an odd prime. Then

$$x^p - x = x(x^{p-1}-1) = x\underbrace{(x^{\frac{p-1}{2}}-1)}_{\text{Roots: all (nonzero) squares in } \mathbb{F}_p}\underbrace{(x^{\frac{p-1}{2}}+1)}_{\text{Roots: all nonsquares in } \mathbb{F}_p} = \underbrace{x(x-1)(x-2)\cdots(x-(p-1))}_{\text{Every } a\in\mathbb{F}_p \text{ is a root of } x^p-x. \text{ (Fermat's Little Theorem)}}$$

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,

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

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

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

So $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod 13.$

eg. $\left(\frac{7}{13}\right) = -1$ $\left(\frac{0}{13}\right) = 0$ $\left(\frac{39}{3}\right) = 0$ $\left(\frac{20}{13}\right) = -1$

$\left(\frac{10}{13}\right) = 1$

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all $a, b \in \mathbb{Z}$ (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 $20 \equiv 7 \bmod 13$ is a nonsquare mod 13.

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

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

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

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

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

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

We can use Euler's Criterion $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$. 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).

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

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

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

eg. $\left(\frac{2}{7}\right) = 1$ since $2 \equiv 3^2 \bmod 7$

$7 \equiv -1 \bmod 8$ 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:

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

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

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 $47 \equiv -1 \bmod 8$ Since $7 \equiv 47 \equiv 3 \bmod 4$

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

$89 \equiv 1 \bmod 4$ i.e. 60 is a nonsquare mod 89.

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

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

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

If $\left(\frac{c}{p}\right) = -1$ (c is nonsquare mod p) take $x \equiv c^{\frac{p-1}{4}} \bmod p$, then $x^2 \equiv c^{\frac{p-1}{2}} \equiv -1 \bmod p$

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 $x^2 \equiv -1 \bmod p$.

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

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

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 mod p are $\pm\frac{a}{b}$.

Theorem Let p be prime. Then p is a sum of two squares iff $p \not\equiv 3 \mod 4$.

Proof We already know that if $p \equiv 3 \mod 4$ then p is not a sum of two squares. Conversely, suppose p is prime, $p \not\equiv 3 \mod 4$. There is more than one proof but we will give an algorithm solution which tells us how to find $a, b \in \mathbb{Z}$ such that $a^2+b^2 = p$. This algorithm is very efficient in practice even for primes having hundreds or thousands of decimal digits. If $p=2$ then $p = 1^2+1^2$. Henceforth $p \equiv 1 \mod 4$. Let $c \in \{1, \dots, p-1\}$ such that $c^2 \equiv -1 \mod p$. (See previous slide for a method to find c.) Then $c^2+1 \equiv 0 \mod p$ i.e. $c^2+1 = mp$ for some $m \geq 1$. We can iterate the ~~following~~ descent step which leads from a large multiple of p as $\square^2 + \square^2$, to a smaller multiple of p of this form, repeating until we get $p = a^2+b^2$, $a, b \in \mathbb{Z}$.

(Fermat's Method of Descent)

Suppose $mp = a^2+b^2$, $a,b \in \{\pm 1, \pm 2, \cdots, \pm \frac{p-1}{2}\}$. So $mp = \alpha\bar{\alpha}$, $\alpha = a+bi \in \mathbb{Z}[i]$

After reducing a,b mod m to get $\alpha \equiv \beta \mod m$ where $\beta = a'+b'i$, $|a'|, |b'| \leq \frac{m}{2}$ (choose $a', b' \in \{-\frac{m}{2}, \dots, \frac{m}{2}\}$ or $\{\frac{-m+1}{2}, \dots, \frac{m-1}{2}\}$)

$a \equiv a' \mod m$

$b \equiv b' \mod m$

Then $\alpha\bar{\beta} = m\gamma$ for some $\gamma \in \mathbb{Z}[i]$.

since $\alpha\bar{\beta} = (a+bi)(a'-b'i) = \underbrace{(aa'+bb')}_{\substack{\equiv a^2+b^2 = mp \\ \equiv 0 \mod m}} + \underbrace{(a'b-ab')}_{\equiv ab-ab \equiv 0 \mod m}i$

$\alpha\bar{\alpha} = mp$

$\alpha\bar{\alpha}\beta\bar{\beta} = mp\beta\bar{\beta}$

$(\alpha\bar{\beta})\overline{(\alpha\bar{\beta})} = mp\beta\bar{\beta}$

$m\gamma \cdot m\bar{\gamma} = mp\beta\bar{\beta}$

$m\gamma\bar{\gamma} = p\beta\bar{\beta}$ where p divides both sides so $\gamma\bar{\gamma} = pk$

$mpk = p\beta\bar{\beta}$

$mk = \beta\bar{\beta}$

$m^2\gamma\bar{\gamma} = mp\beta\bar{\beta} = mp \cdot mk$

$\gamma\bar{\gamma} = pk$. where we can check $1 \leq k < m$.

This can be checked carefully to finish the proof.

Eg. Write $p=1009$ as a sum of two squares. ($1009 \equiv 1$ prime)

$2^{\frac{p-1}{2}} \equiv 1 \mod p$ so $\left(\frac{2}{p}\right) = 1$

$13^{\frac{p-1}{2}} \equiv -1 \mod p$ so $13, 31$ nonsquares mod $p = 1009$.

$31^{\frac{p-1}{2}} \equiv -1 \mod p$

$13^{\frac{p-1}{4}} \equiv 469 \mod p$

$31^{\frac{p-1}{4}} \equiv 540 \mod p$

The two square roots of -1 mod p are ± 469 i.e. $469, 540$.

Choosing the smallest nonsquare

$469 \leq \frac{p-1}{2}$

$469^2 + 1^2 = \underbrace{218}_{m} p$, $\alpha = 469 + i$, $\beta = 33 + i$

$469 \equiv 33 \mod 218$

$1 \equiv 1 \mod 218$

$\cancel{m}\gamma = \alpha\bar{\beta} = (469+i)(33-i) = 15478 - 436i = \cancel{218}(71-2i)$

$\gamma = 71 - 2i$

$\gamma\bar{\gamma} = 71^2 + 2^2 = 5045 = 5p$

Repeat the descent step starting with $71^2 + 2^2 = \underbrace{5}_{m}p$, $\alpha = 71 + 2i$, $\beta = 1 + 2i$ mod m

$m\gamma = \alpha\bar{\beta} = (71+2i)(1-2i) = 75 - 140i = 5(15-28i)$

$\gamma = 15 - 28i$

$\gamma\bar{\gamma} = 15^2 + 28^2 = 1009 = p$