



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

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

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  $\pm \frac{a}{b}$ .

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

Proof We already know that if  $p \equiv 3 \pmod{4}$  then  $p$  is not a sum of two squares. Conversely, suppose  $p$  is prime,  $p \not\equiv 3 \pmod{4}$ . 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  $p \equiv 1 \pmod{4}$ . Let  $c \in \{1, \dots, p-1\}$  such that  $c^2 \equiv -1 \pmod{p}$ . (See previous slide for a method to find  $c$ .) Then  $c^2 + 1 \equiv 0 \pmod{p}$  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  $mp = a^2 + b^2$ ,  $a, b \in \{\pm 1, \pm 2, \dots, \pm \frac{p-1}{2}\}$ . So  $mp = \alpha \bar{\alpha}$ ,  $\alpha = a + bi \in \mathbb{Z}[i]$ . After reducing  $a, b \pmod{m}$  to get  $\alpha \equiv \beta \pmod{m}$  where  $\beta = a' + bi$ ,  $|a'|, |b'| \leq \frac{m}{2}$  (choose  $a', b' \in \{\frac{-m}{2}, \dots, \frac{m}{2}\}$  or  $\{\frac{m+1}{2}, \dots, \frac{m-1}{2}\}$ ). Then  $\alpha \bar{\beta} = m\gamma$  for some  $\gamma \in \mathbb{Z}[i]$ .

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

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

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

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

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

$$m\gamma \bar{\gamma} = p \beta \bar{\beta}$$

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

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

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

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

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

This can be checked carefully to finish the proof.

Eg. Write  $p=1009$  as a sum of two squares. ( $1009 \equiv 1 \pmod{4}$  prime)

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

$$13^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

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

so 13, 31 nonsquares mod  $p=1009$ .

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

$$31^{\frac{p-1}{4}} \equiv 570 \pmod{p}$$

The two square roots of  $-1 \pmod{p}$  are  $\pm 469$  i.e. 469, 570.

Choosing the smallest nonsquare

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

$$469^2 + 1^2 = \underbrace{218}_m p$$

$$\alpha = 469 + i$$

$$\beta = 33 + i$$

$$469 \equiv 33 \pmod{218}$$

$$1 \equiv 1 \pmod{218}$$

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

$$\gamma = 71 - 2i$$

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

Repeat the descent step starting with  $71^2 + 2^2 = \underbrace{5}_m p$ ,

$$\alpha = 71 + 2i \pmod{m}$$

$$\beta = 1 + 2i \pmod{m}$$

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

$$\gamma = 15 - 28i$$

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

Which positive integers have the form  $a^2 + b^2$  ( $a, b \in \mathbb{Z}$ )?

We know the answer for a prime number  $p$ :  $p$  is a sum of two squares iff  $p=2$  or  $p \equiv 1 \pmod{4}$ .

For general  $n$ ,

$$n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4} 11^{k_5} 13^{k_6} 17^{k_7} \dots$$

(all exponents are zero eventually)

eg.  $n = 2^5 3^4 5^3 7^3 11^1 13^1 17^0 19^2 23^0 29^0 31^0 37^0 \dots = 2^5 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 11 \cdot 13 \cdot 19^2$  is a sum of two squares.

$$\begin{array}{c} 2^* \quad \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ 2^5 \quad 3^4 \quad 5^3 \quad 7^3 \quad 11 \quad 13 \quad 19^2 \\ \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ 2^* \quad 9^2 \quad 5^* \quad (7^3)^2 = (7^3)^2 + 0^2 \\ \uparrow \quad \uparrow \quad \uparrow \\ 2^* \quad 9^2 \quad 5^* \end{array}$$

If the exponent on every prime  $\equiv 3 \pmod{4}$  is even, then  $n$  is a sum of two squares; the converse is true, if some prime  $p \equiv 3 \pmod{4}$  has odd exponent,  $n$  cannot be a sum of two squares.

21 is not a sum of two squares. (0, 1, 4, 9, 16 are the only squares  $< 21$ )

"3 · 7". This can all be proved using the idea presented in the previous class.

In order to be able to write  $n$  as a sum of two squares, it needs to be small enough or we need to know its prime factorization.

Writing a number as a sum of two squares is as hard as integer factorization. Factorization in  $\mathbb{Z}[i]$  is the same problem as writing a number as a sum of two squares.

Next: Public Key Cryptography, especially

- Diffie-Hellman
- RSA (Rivest-Shamir-Adleman)

First: primitive elements in finite fields

Let  $p$  be prime,  $\mathbb{F}_p =$  field of order  $p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ .

Fact:  $\mathbb{F}_p$  has a primitive element  $g \in \mathbb{F}_p$ , namely all nonzero elements of  $\mathbb{F}_p$  are powers of  $g$ , i.e.  $\mathbb{F}_p = \{0, 1, g, g^2, g^3, \dots, g^{p-2}\}$  ( $g^{p-1} = 1$  by Fermat's Little theorem).

eg.  $\mathbb{F}_7$  has 3 as a primitive element:  $\mathbb{F}_7 = \{0, 1, \underset{2}{3}, \underset{6}{3^2}, \underset{4}{3^3}, \underset{5}{3^4}, 3^5\}$

Also  $5 = 3^4$  is also a primitive element of  $\mathbb{F}_7$ :  $\mathbb{F}_7 = \{0, 1, \underset{4}{5}, \underset{6}{5^2}, \underset{2}{5^3}, \underset{3}{5^4}, 5^5\}$

2 is not primitive: powers of 2 are 1, 2, 4 only.

More generally, for every prime power  $q = p^k$ ,  $p$  prime,  $k \geq 1$ .  $\mathbb{F}_q$  (field of order  $q$ ) always has a primitive element).

Why?  $\mathbb{F}_5$  has multiplicative group  $\mathbb{F}_5^* = \{1, 2, 3, 4\}$  which cannot be a Klein 4-group, otherwise of degree 2 having four roots in  $\mathbb{F}_5$ .

$x^2 = 1$  for every nonzero  $a \in \mathbb{F}_5$  but then  $x^2 - 1$  is a polynomial

So  $\mathbb{F}_5^*$  must be cyclic.

eg.  $\mathbb{F}_{1009} = \{0, 1, 11, \dots, 1008\} = \{0, 1, 11, 11^2, 11^3, \dots, 11^{1007}\}$   
 $= \{0, 1, 11, 121, 322, 515, 620, \dots, 367\}$

1009 is prime

11 is a primitive (I checked using Mathematica)

$11^k = 186$        $k$  is the "discrete logarithm" of 186 (base 11)      not  $\log_{11} 186 = \frac{\ln 186}{\ln 11}$

Answer:  $k = 543$

$11^{543} = 186$  in  $\mathbb{F}_{1009}$       i.e. in  $\mathbb{Z}$ ,  $11^{543} \equiv 186 \pmod{1009}$ .

Discrete logs and integer factorization are two difficult computational tasks.

That's good! Since this provides a secure cryptosystem for key exchange.

Alice and Bob want to agree on a large integer to be used as the encryption key for a word document (or other symmetric key encryption algorithm) ("symmetric" means that the decryption key is the same as the encryption key).

Diffie-Hellman Key exchange protocol: Alice and Bob communicate over an open (insecure) channel. They first agree on a large prime  $p$ . (Eg. Alice can generate  $p$  and send it to Bob over the open channel.) Next, they agree on a primitive element  $g$  for  $\mathbb{F}_p$ . (A random element is almost as good.) One party can obtain  $g$  and send it to the other party.

Alice chooses  $a \in \{2, 3, \dots, p-2\}$  randomly and she computes  $g^a \pmod p$ . She sends this to Bob.

Bob chooses  $b \in \{2, 3, \dots, p-2\}$  and he computes  $g^b \pmod p$ . He sends this to Alice.

Eve (an eavesdropper) knows  $p, g, g^a \pmod p, g^b \pmod p$ . (But not  $a, b$ .)

$p, g, g^a \pmod p, g^b \pmod p$  Public key

The shared secret key is  $g^{ab} \pmod p$ .  
 Bob computes  $(g^a)^b \equiv g^{ab} \pmod p$ .

## Fair Coin Flip

Alice generates  $p, q$  primes generated randomly but  $\begin{cases} p \equiv q \equiv 1 \pmod{4} \\ \text{or} \\ p \equiv q \equiv 3 \pmod{4} \end{cases}$  if a coin flip is H  
- - - - - T

Alice sends  $n = pq$  to Bob.  
Bob guesses H or T.

$$n \equiv 1 \pmod{4}.$$

Bob verifies  $n \equiv 1 \pmod{4}$ , prime.