TOPIC: 6.857

DATE: 3/2/22

FILE UNDER:

PAGE: L10

Admin:

Projects

Today:

Group Theory Z_p^*, Q_p, Z_n^*, Q_n, Elliptic curves

Finding primes & generators

Finite Fields $GF(p^k)$

Secret Sharing

Readings:

Katz/Lindell Ch. 8

Paar/Pelzl Ch 6,7,8,9

TOPIC:

DATE:

FILE UNDER:

Group Theory review:

(multiplicative group) If $(G, *)$ is a finite abelian group of size t:

identity
- $\exists$ identity 1 s.t. $(\forall a \in G)\ a \cdot 1 = 1 \cdot a = a$

inverses
- $(\forall a \in G)(\exists b \in G)\ a \cdot b = 1 \qquad (b = a^{-1})$

associativity
- $(\forall a, b, c \in G)\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

commutativity
- $(\forall a, b \in G)\ a \cdot b = b \cdot a$

order

Let order(a) = least $u > 0$ s.t. $a^u = 1$ (in G).

Theorem: In a finite abelian group of size t

$$(\forall a \in G)\ \text{order}(a) \mid t.$$

Theorem: In a finite abelian group of size t

$$(\forall a \in G)\ a^t = 1$$

Example: $(\forall a \in \mathbb{Z}_p^*)\ a^{p-1} = 1 \pmod p$ since $|\mathbb{Z}_p^*| = p-1$.

Def: $\langle a \rangle = \{a^i : i \geq 0\}$ = subgroup generated by a

Def: If $\langle a \rangle = G$ then G is cyclic and a is a generator of G.

Note: $|\langle a \rangle| = \text{order}(a)$

Exercise: In a finite abelian group G of order t, where t is prime, $(\forall a \in G)\ [a \neq 1] \Rightarrow [a \text{ is a generator of } G]$.

Fact: $\mathbb{Z}_p^*$ is always cyclic.

TOPIC:

DATE:

FILE UNDER:

- Fact: If G is a cyclic group of order t and generator g, then the relation $x \longleftrightarrow g^x$ is one-to-one between $[0,1,\dots,t-1]$ and G.

  $x \longmapsto g^x$: exponentiation, "powering-up"

  $g^x \longmapsto x$: discrete logarithm (DL)

- Computing discrete logarithms (the DL problem) is commonly assumed to be hard/infeasible for well-chosen groups G. [E.g. Z_p^* for p a large randomly chosen prime]

- We often need to be able to represent messages as group elements: if M is a message space & G a group, we need an injective (one-to-one) map

  $$f : M \longrightarrow G$$

  such that $f(m)$ can be chosen to "represent" message m.

  E.g. if $p > 2^k$ then we can identify k-bit messages with the integers $1, 2, \dots, 2^k \bmod p$ (in Z_p^*).

  In some groups this can be a little tricky.

TOPIC:

DATE:

FILE UNDER:

PAGE: L14.4

We look at five commonly used finite groups.

① $Z_p^* = \{a : 1 \le a < p\}$ where p is prime

Z_p^* is always cyclic.

If $p = 2q+1$ (q prime), then p is a "safe prime" and half of Z_p^* are generators, and the other half are squares (Q_p).

② Q_p = quadratic residues (squares) mod prime p

$= \{a^2 : 1 \le a < p\}$

$\subsetneq Z_p^*$

$|Q_p| = \frac{1}{2}|Z_p^*| = (p-1)/2$ ("half of Z_p^* are squares".

Q_p is cyclic: If $\langle g\rangle = Z_p^*$, then $\langle g^2\rangle = Q_p$.

$Q_p = \{g^{2i} : 0 \le i < (p-1)/2\}$ if $\langle g\rangle = Z_p^*$.

If $p = 2q+1$ (p is a "safe prime") then

$|Q_p| = q$

and any element of Q_p (other than 1) generates Q_p. [To find a generator, take the square of any element $a \notin \{1, p-1\}$.]

TOPIC:

FILE UNDER:

DATE:

(3) $Z_n^* = \{a : \gcd(a,n)=1 \ \& \ 1 \le a < n\}$

$|Z_n^*| = \varphi(n)$ [by defn]

If $n = p \cdot q$ where p, q distinct odd primes,

then Z_n^* is not cyclic

$$Z_n^* \approx Z_p^* \times Z_q^* \quad \text{(Chinere remainder thm)}$$

(4) $Q_n = \{a^2 : 1 \le a < n \ \& \ \gcd(a,n) = 1\}$

= "squares mod n"

= "quadratic residues mod n"

If $n = p \cdot q$ where

$p = 2r+1$ is a safe prime (r prime)

$q = 2s+1$ is a safe prime (s prime)

then

$|Q_n| = r \cdot s$

& Q_n is cyclic.

(5) Elliptic curve groups

Quite different, many nice properties, widely used.

Much deep mathematics related to elliptic curves.

Here is a very brief intro.

Let p be a prime.

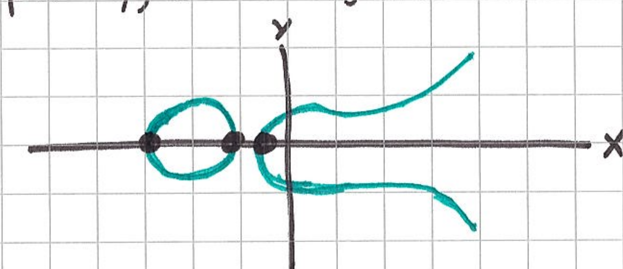
Let a, b be elements of Z_p such that

$$4a^3 + 27b^2 \neq 0 \pmod p \qquad (*)$$

Consider equation (in variables x, y mod p)

$$y^2 = x^3 + ax + b \pmod p \qquad (**)$$

Graphically, something like this



Note that if (x, y) on curve, so is $(x, -y)$.

If roots are r_1, r_2, r_3 then

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4a^3 + 27b^2)$$

so $(*)$ means roots are distinct.

TOPIC:

DATE:

FILE UNDER:

Def: The points on the curve (**) are

$$E = \{ (x,y) : y^2 = x^3 + ax + b \pmod p \} \cup \{\infty\}$$

Here "∞" denotes the "point at infinity" (e.g. $y = \infty$)

Fact: $|E| = p + 1 + t$ where $|t| \leq 2\sqrt{p}$

(This is about what you'd expect if $x^3 + ax + b$ acted "randomly": about half the values are squares, each of which has two square roots.)

Fact: $|E|$ can be compted "efficiently".

(Surprising) **Fact:** A binary operation (written additively as "+" can be defined on E s.t. $(E, +)$ is a finite abelian group.

[∞ is the identity: $P + \infty = \infty + P = P$

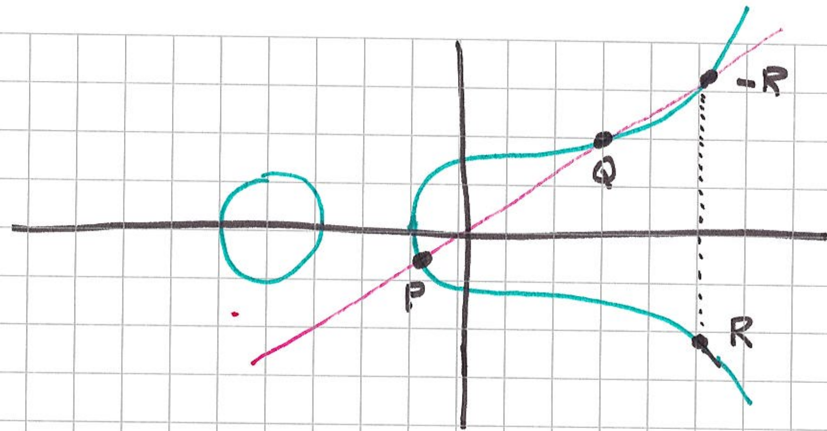
[The inverse of (x,y) is $(x,-y)$ [also on curve].

[The inverse of ∞ is ∞.

TOPIC:

DATE:

FILE UNDER:



Let $P = (x_1, y_1)$ $Q = (x_2, y_2)$ $R = P+Q = (x_3, y_3)$.

Roughly: PQ defines a line.
Find "other point" on this line (call it $-R$)
return R as $P+Q$

Code: If $x_1 \neq x_2$: $m = (y_2 - y_1)/(x_2 - x_1)$ ("slope")

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

If $x_1 = x_2$ & $y_1 \neq y_2$: $P+Q = \infty$ (vertical line)

If $P = Q$ & $y_1 = 0$: $P+Q = \infty$ (vertical tangent)

If $P = Q$ & $y_1 \neq 0$: $m = (3x_1^2 + a)/2y_1$ (tangent)

$$x_3 = m^2 - 2x_1$$

$$y_3 = m(x_1 - x_3) - y_1$$

Theorem: "+" is associative binary operation on E. (!)

Cor: (E, +) is a finite abelian group.

Fact: (E, +) may or may not be cyclic.

Fact: Can use other finite fields (e.g. $GF(2^k)$) instead of $\mathbb{F}_p$.

TOPIC:

DATE:

FILE UNDER:

Why are elliptic curves interesting?

- The discrete logarithm problem seems to be quite <u>hard</u> (requiring $\approx |E|^{1/2}$ steps) for well-chosen E. (See "NIST standard curves")
  Thus, the groups can be <u>smaller</u> than Z_p^* of the same security level. This yields both <u>compactness</u> and <u>efficiency</u>.
- Some elliptic curves admit "bilinear maps" enabling all sorts of really wonderful crypto operations. (More on this later.)

TOPIC:

DATE:

FILE UNDER:

- How to find large (k-bit) random prime #?

  Generate & test: do $p \leftarrow$ random k-bit integer

  until p is prime

- Works because primes are "dense":

  about $2^k / \ln(2^k)$ k-bit primes (Prime Number Theorem)

  $\Rightarrow$ one of every $\approx 0.69k$ k-bit integers is prime.

- To test if a large randomly-chosen k-bit integer is prime, it suffices to test

$$2^{p-1} \stackrel{?}{=} 1 \pmod{p}$$

  - This works with high probability (w.h.p) for random p; doesn't work for adversarially chosen p.
  - See CLRS for Miller-Rabin primality test (randomized)
  - Technically, above gives "base-2 pseudoprime", but this is almost always prime
  - $\exists$ deterministic poly-time primality test (Agrawal, Kayal, Saxena 2002):

    Test $(x-a)^p = x^p - a \pmod{p}$ $\quad$ x variable

    which is true iff p is prime

    Test mod p & mod $x^r - 1$ for small r & small a's.

Order of elements (in Z_p^* or Z_n^*):

Define: $\text{order}_n(a)$ = "order of a, modulo n"

$= \text{least } t>0 \text{ s.t. } a^t \equiv 1 \pmod n$

Recall Fermat's Little Theorem:

If p prime, then $(\forall a \in Z_p^*)\ a^{p-1} \equiv 1 \pmod p$

For general n, we have Euler's Theorem:

$(\forall n)(\forall a \in Z_n^*)\ a^{\varphi(n)} \equiv 1 \pmod n$

where $Z_n^* = \{a : \gcd(a,n) = 1\}$

= multiplicative group modulo n

$\varphi(n) = |Z_n^*|$

Example: $Z_{10}^* = \{1, 3, 7, 9\}$

$\varphi(10) = 4$

$3^4 \equiv 1 \pmod{10}$

Thus $\varphi(n)$ is well-defined for all n, &

$\text{order}_n(a)$ is also well-defined.

Can we say more?

Example: mod $p = 7$

	1	2	3	4	5	6	7 ...	
1	1	1	1	1	1	1	1 ...	order(1) = 1
2	2	4	1	2	4	1	2 ...	order(2) = 3
3	3	2	6	4	5	1	3 ...	order(3) = 6
4	4	2	1	4	2	1	4 ...	order(4) = 3
5	5	4	6	2	3	1	5 ...	order(5) = 6
6	6	1	6	1	6	1	6 ...	order(6) = 2

Fermat

Def: $\langle a \rangle = \{a^i : i \geq 0\}$ = subgroup generated by a

Example: $\langle 2 \rangle = \{2, 4, 1\}$ (in $\mathbb{Z}_7^*$)

Theorem: $\text{order}(a) = |\langle a \rangle|$

Theorem: If p prime: $\text{order}_p(a) \mid (p-1)$.

Theorem: $|\langle a \rangle| \;\big|\; |\mathbb{Z}_n^*|$

or: $\text{order}_n(a) \mid \varphi(n)$ equivalently.

Generators

Def: If $\text{order}_p(g) = p-1$

then g is a generator of Z_p^*.

(i.e. $\langle g \rangle = Z_p^*$)

Theorem: If p is a prime and

g is a generator mod p, then

$$g^x = y \pmod{p}$$

has a <u>unique</u> solution x $(0 \le x < p-1)$

for each $y \in Z_p^*$.

Def: x is the "discrete logarithm"

of y, base g, modulo p.

x =	1	2	3	4	5	6
g^x =	3	2	6	4	5	1

for $g = 3$, modulo 7

Theorem: $\mathbb{Z}_n^*$ has a generator
(i.e. $\mathbb{Z}_n^*$ is <u>cyclic</u>)
iff n is
2, 4, p^m, or $2p^m$
for some prime p & $m \geq 1$.

Theorem: If p is prime, the number of generators mod p is $\varphi(p-1)$

Example: $p = 11$
$\mathbb{Z}_{11}^*$ has $\varphi(10) = 4$ generators
(they are $2, 6, 7,$ and 8).

<u>How to find a generator mod a prime p?</u>

In general, seems to require knowledge of factorization of $p-1$.

While factoring is hard, we can <u>create</u> primes for which factoring $p-1$ is trivial.

Def: If p & q are both primes &

$$p = 2q + 1$$

then p is a "safe prime" and

q is a "Sophie Germain prime".

Examples: $p = 23$, $q = 11$ $\quad$ $p = 11$, $q = 5$

$p = 59$, $q = 29$ $\quad$ ...

Theorem: If p is a safe prime

then $p - 1 = 2 \cdot q$

so $(\forall a \in \mathbb{Z}_p^*)$ $\text{order}_p(a) \in \{1, 2, q, 2q\}$.

It is not hard to find safe primes. ("Probability" that a prime p is safe is $\approx 1/\ln^2(p)$, empirically.)

Can test if g is a generator mod $p = 2q + 1$ easily:

check that $g^{p-1} = 1 \pmod p$ $\quad$ ✓ by Fermat

& $g^2 \neq 1 \pmod p$ $\quad$ $[\text{order}_p(g) \neq 2]$

& $g^q \neq 1 \pmod p$ $\quad$ $[\text{order}_p(g) \neq q]$

then $\text{order}_p(g) = p - 1$.

We can use "generate & test" again: (for "safe prime" p)

do $g \xleftarrow{R} \mathbb{Z}_p^*$

until $\text{order}_p(g) = p-1$

Generators are quite common:

Theorem: If $p = 2q+1$ is a "safe prime"

then # generators mod p

$= \varphi(p-1)$

$= q-1$ (almost half of them!)

(In general:

Theorem: If p prime, then

generators mod p

$= \varphi(p-1)$

$\geq \dfrac{p-1}{6 \ln\ln(p-1)}$

)

So generate & test works well for finding generators modulo a safe prime p, or modulo any prime p for which you know $\varphi(p-1)$.

Notation: $GF(q)$ is <u>the</u> finite field ("Galois field") with q elements

Theorem: $GF(q)$ exists whenever

$$q = p^k, \quad p \text{ prime}, \quad k \geq 1$$

Two cases:

① $GF(p)$ – work modulo prime p

Z_p = integers mod p = $\{0, 1, \ldots, p-1\}$

$Z_p^* = Z_p - \{0\} = \{1, 2, \ldots, p-1\}$

② $GF(p^k)$: $k > 1$

work with polynomials of degree $< k$
with coefficients from $GF(p)$
modulo fixed irreducible polynomial of degree k

Common case is $GF(2^k)$

Note: all operations can be performed efficiently (inverses to be demonstrated)

Finite fields: System $(S, +, \circ)$ s.t.

- S is a finite set containing "0" & "1"
- $(S,+)$ is an abelian (commutative) group with identity 0

group laws
$$\left[\begin{array}{ll} ((a+b)+c) = (a+(b+c)) & \text{associative} \\ a+0 = 0+a = a & \text{identity } 0 \\ (\forall a)(\exists b)\ a+b=0 & \text{(additive) inverses } b=-a \end{array}\right.$$

$a+b = b+a$ commutative

- $(S^*, \circ)$ is an abelian group with identity 1

S^* = nonzero elements of S

group laws
$$\left[\begin{array}{ll} (a\circ b)\circ c = a\circ(b\circ c) & \text{associative} \\ a\circ 1 = 1\circ a = a & \text{identity } 1 \\ (\forall a \in S^*)(\exists b \in S^*)\ a\circ b = 1 & \text{(multiplicative inverses) } b = a^{-1} \end{array}\right.$$

$a\circ b = b\circ a$ commutative

- Distributive laws: $a\circ(b+c) = a\circ b + a\circ c$

$(b+c)\circ a = b\circ a + c\circ a$ (follows)

Familiar fields: $\mathbb{R}$ (reals) are infinite

$\mathbb{C}$ (complex)

For crypto, we're usually interested in finite fields, such as $\mathbb{Z}_p$ (integers mod prime p)

Over field, usual algorithms work (mostly).

E.g. solving linear eqns:

$$ax + b = 0 \pmod{p}$$

$$\Rightarrow \quad x = a^{-1} \cdot (-b) \pmod{p} \quad \text{is soln.}$$

$$3x + 5 = 6 \pmod{7}$$

$$3x = 1 \pmod{7}$$

$$x = 5 \pmod{7}$$

Construction of $GF(2^2) = GF(4)$

Has 4 elements.

Is not arithmetic mod 4. (where 2 has no mult inverse)

elements are polynomials of ~~degree~~ degree < 2 with coefficients mod 2 (i.e. in $GF(2)$):

		x	1
0		0	0
1		0	1
x		1	0
$x+1$		1	1

Addition is component-wise according to powers, as usual

$$(x) + (x+1) = (2x+1) = 1 \quad (\text{coefs. mod } 2)$$

Multiplication is modulo x^2+x+1
which is irreducible (doesn't factor)

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 \bmod (x^2+x+1)$ is $x+1$ (note that $x \equiv -x$ coefs mod 2)

Key management

Start with "secret sharing" (threshold cryptography).

- Assume Alice has a secret s. (e.g. a key)
- She wants to protect s as follows:

  She has n friends $A_1, A_2, \ldots, A_n$

  She picks a "threshold" t, $1 \le t \le n$.

  She wants to give each friend A_i,

  a "share" s_i of s, so that

  - any t or more friends can reconstruct s
  - any set of $< t$ friends can not.

Also see bitcoin "multisig" as motivation

Easy cases:

$t = 1$: $s_i = s$

$t = n$: $s_1, s_2, \ldots, s_{n-1}$ random

s_n chosen so that

$$s = s_1 \oplus s_2 \oplus \cdots \oplus s_n$$

What about $1 < t < n$?

Shamir's method ("How to Share a Secret", 1979)

Idea: 2 points determine a line
3 points determine a quadratic
...
t points determine a degree $(t-1)$ curve

Let $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + a_0$

There are t coefficients. Let's work modulo prime p.

We can have t points: (x_i, y_i) for $1 \le i \le t$

They determine coefficients, and vice versa.

$$\begin{tikzcd}[column sep=huge] \{(x_i, y_i)\} \arrow[r, bend right, "\text{Polynomial Interpolation}"'] & (a_{t-1}, a_{t-2}, \ldots, a_1, a_0) \arrow[l, bend right, "\text{Polynomial Evaluation}"'] \end{tikzcd}$$

Pt/value pairs — Coefficients

To share secret s (here $0 \le s < p$):

Let $y_0 = a_0 = s$

Pick $a_1, a_2, \ldots, a_{t-1}$ at random from $\mathbb{Z}_p$

Let share $s_i = (i, y_i)$ where $y_i = f(i)$, $1 \le i \le n$.

Evaluation is easy.

Interpolation

Given (x_i, y_i) $\quad 1 \le i \le t \quad$ (wlog)

Then $f(x) = \sum_{i=1}^{t} f_i(x) \cdot y_i$

where $f_i(x) = \begin{cases} 1 & \text{at } x = x_i \\ 0 & \text{for } x = x_j,\ j \ne i,\ 1 \le j \le t \end{cases}$

Furthermore:

$$f_i(x) = \frac{\prod_{j \ne i} (x - x_j)}{\prod_{j \ne i} (x_i - x_j)}$$

This is a polynomial of degree $t-1$. So f also has degree $t-1$.

Evaluating $f(0)$ to get s simplifies to

$$s = f(0) = \sum_{i=1}^{t} y_i \cdot \frac{\prod_{j \ne i} (-x_j)}{\prod_{j \ne i} (x_i - x_j)}.$$

Theorem: Secret sharing with Shamir's method is information-theoretically secure. Adversary with $< t$ shares has no information about s.

Pf: A degree $t-1$ curve can go through any point $(0, s)$ as well as any given d pts (x_i, y_i), if $d < t$. $\boxed{\checkmark}$

Refs: Reed-Solomon codes, erasure codes, error correction, information dispersal (Rabin).