The Discrete Logarithm and Integer Order

have modulus p
integers g & A

find: x s.t. $g^x \equiv A \bmod p$.

in $\mathbb{R}$:
$\log_a b = x \iff a^x = b$
(cts logarithm)

In $\mathbb{Z}/m\mathbb{Z}$
$\log_a b = x \iff a^x \equiv b \bmod m$
$\operatorname{ind}_a b$

In $\mathbb{Z}/8\mathbb{Z}$
$\log_2 5$ DNE

In $\mathbb{Z}/7\mathbb{Z}$
$\log_2 5$ DNE
$2^1 = 2$
$2^2 = 4$
$2^3 \equiv 1$
$2^4 \equiv 2$
$2^5 \equiv 4$
$2^6 \equiv 1$

Dfn: $m \in \mathbb{Z}^{>0}$
We say $a \in \mathbb{Z}/m\mathbb{Z}$ is a unit mod m
if a has an inverse mod m.
(iff $\gcd(a, m) = 1$).
We say $a \in (\mathbb{Z}/m\mathbb{Z})^\times$

If p is prime
$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, 3, \ldots, p-1\}$

Fermat's Little Theorem

Let p be prime:

$\gcd(a,p) = 1$.

Then $a^{p-1} \equiv 1 \bmod p$.

(equivalently

$a^p \equiv a \bmod p$)

$2^6 \equiv 1 \bmod 7$

$2^6 = 64 = 7 \cdot 9 + 1 \equiv 1 \bmod 7$

$3^6 = 1 \bmod 7$

$3^2 = 9 \equiv 2$

$3^3 \equiv 6$

$3^4 \equiv 4$

$3^5 \equiv 5$

$3^6 \equiv 1$.

If $3^x \equiv 1$ then $x \geq 6$

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^3 = 8 \equiv 1$.

Dfn: $g \in \mathbb{Z}/p\mathbb{Z}$ is a primitive root mod p if

$\{g, g^2, g^3, \cdots, g^{p-1}\} = \mathbb{Z}/p\mathbb{Z}^\times$

In this case, there are no repetitions

$g^x \equiv 1$ for $x < p-1$.

mod 7

$3, 3^2, 3^3, 3^4, 3^5, 3^6$

3 2 6 4 5 1

$2, 2^2, 2^3, 2^4, 2^5, 2^6$

2 4 1 2 4 1

---

mod 11

2 4 8 5 10 9 7 3 6 1

is a PR

$10 \quad 10^2 \equiv 1 \quad 10^3 = 10 \quad 10^4 = 1,$

10, 1, 10, 1, 10, 1

not a PR

Fact: If $g \in \mathbb{Z}/p\mathbb{Z}^\times$

then $\#\{g^i \bmod p \mid 1 \le i \le p-1\} \mid p-1$.

in particular, if we compute

$g, g^2, g^3, \dots, g^{\frac{p-1}{2}}$

and haven't gotten 1, then

g is a PR.

Fact: • $\log_g(1) = 0$

• $\log_g(ab) \equiv \log_g(a) + \log_g(b) \bmod p-1$

• $\log_g(a^r) \equiv r \log_g(a) \bmod p-1$.

if $g^a \equiv g^b \bmod p$

$g^{a-b} \equiv 1 \bmod p$

Dfn: p prime

g a PR mod p

$h \in \mathbb{Z}/p\mathbb{Z}^\times$.

If $x \in \mathbb{N}$

$g^x \equiv h \bmod p$

we say x is a discrete log of h to the base g mod m.

(or the index of h wrt g).

The DL is the smallest one.

If $g^x \equiv h \bmod p$

then $g^{x+n(p-1)} \equiv g^x (g^{p-1})^n$

$\equiv g^x \cdot 1^n$

$\equiv g^x \equiv h \bmod p$.

So log only defined mod $p-1$.

take value $0 \le x \le p-2$.

---

2 is a PR mod 11

$\log_2(6) = 9$.

---

2 is PR mod 29.

$\log_2(7) = 12$.

32 64 128 ---

2 4 8 16 3 6 12 24 19 9 18 7

The Order of an integer

Dfn: Let $m \in \mathbb{Z}^{>0}$.

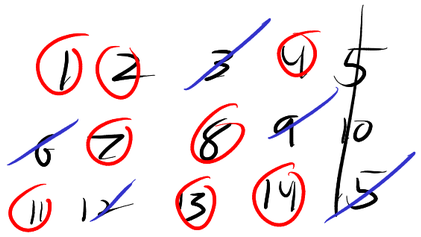
Then the Euler Totient Fn $\phi(m)$ is $\#\ \mathbb{Z}/m\mathbb{Z}^{\times}$

e.g. $\phi(26) = 12$

$\phi(p) = p-1$

$\phi(pq) = (p-1)(q-1)$.

$= pq\left(\frac{p-1}{p}\right)\left(\frac{q-1}{q}\right)$



Thm (Euler): If $a, m \in \mathbb{N}$, $\gcd(a,m)=1$, then

$a^{\phi(m)} \equiv 1 \bmod m$.

Ex: $p=7$, $q=11$,

$\phi(77) = 60$.

$3^{60} = (3^4)^{15} \equiv 4^{15}$

$= (4^3)^5 \equiv (-13)^5$

$= 13^2 \cdot 13^2 \cdot (-13) \equiv 1$.

cor: given a, m, $\gcd(a,m)=1$,

$\exists\ x$ s.t. $a^x \equiv 1 \bmod m$.

Dfn: the order of a is the smallest $x > 0$ s.t.

$a^x \equiv 1 \bmod m$.

$1 \le \mathrm{ord}_m(a) \le \phi(m)$

ex: $\mathrm{ord}_7(2) \equiv 3$

$\mathrm{ord}_7(3) = 6$

$\mathrm{ord}_{10}(3) = 4 = \phi(10)$.