Math 414 Lecture 7: Fermat, Euler, and Wilson

Recall: $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ $\quad \times, +$ mod n

$a \equiv b \pmod n \Leftrightarrow n \mid (a-b)$ $\quad$ equivalence relation

Order of x mod n with $\gcd(x,n)=1$ is:

$\min\{i \geq 1 : x^i \equiv 1 \pmod n\}$

Exists: $x^i \equiv x^j \Rightarrow x^{i-j} \equiv 1$ by cancellation: $ac \equiv bc \pmod n$ and $\gcd(c,n)=1$

$\Rightarrow a \equiv b \pmod n$

Pf: $n \mid ac - bc = (a-b)c$

$\gcd = 1 \Rightarrow n \mid a-b$. ✓

Defn: $\varphi(n) = \#\{a : 1 \leq a \leq n : \gcd(a,n)=1\}$

$\varphi(12) = 4$, $\varphi(p) = p-1$ prime p.

Theorem (Fermat, Euler): If $\gcd(x,n)=1$ then $x^{\varphi(n)} \equiv 1 \pmod n$.

Proof: • Group theory: order of elt. divides order of group

$[x] \in \underbrace{(\mathbb{Z}/n\mathbb{Z})^*}_{\text{Group}} = \{a : 1 \leq a \leq n : \gcd(a,n)=1\}$

• Elementary: $P = \{a : 1 \leq a \leq n : \gcd(a,n)=1\}$

$\overline{P} = \{a \bmod n : a \in P\}$

$\overline{xP} = \{xa \bmod n : a \in P\}$

$\overline{P} = \overline{xP}$ since reduction is injective map (by cancellation).

So $\prod_{a \in P} a \equiv \prod_{a \in P} xa \pmod n$

Cancel: $x^{\#P} \equiv 1 \pmod n$. $\boxed{Z}$

This is critical to public key cryptography!

A terrible primality test!

2010-01-20	②
414	Stein

Theorem (Wilson): $p > 1$ prime $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$

Proof: $p=2$ ✓ So assume $p > 2$.

($\Rightarrow$) p prime

Consider: $1 \quad 2 \quad 3 \quad \cdots \quad p-1$

Observe: $ax \equiv 1 \pmod{p}$

if $x = a$ then $a^2 \equiv 1$ so $p \mid a^2 - 1 = (a-1)(a+1) \Rightarrow a \equiv \pm 1 \pmod{p}$.

So: We pair off elts of $\{2, \ldots, p-2\}$ with their inverses.

$$(p-1)! = 1 \cdot \overbrace{2 \cdot 3 \cdots (p-2)} (p-1)$$

$$\equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$ ✓

($\Leftarrow$) Suppose $(p-1)! \equiv -1 \pmod{p}$.

$\exists\, \ell \mid p$ with $\ell \neq p$ prime $\Rightarrow \ell \nmid (p-1)!$

$\Rightarrow \ell \mid \gcd(p, (p-1)!) = 1.$ ✓

Ex: • $p = 5$.

$(p-1)! = 4! = 24 \equiv -1 \pmod{5}$.

• $p = 6$

$(p-1)! = 5! = 120 \equiv 0 \pmod{6}$.

This is a bad algorithm for primality testing!

Math 414: Lecture 7 (continued)

Chinese Remainder Theorem:

How to (when) solve: $(*)\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ simultaneous linear equations modulo.

Theorem (CRT) If $\gcd(m,n)=1$ then there is a solution x to $(*)$ that is unique modulo mn.

Proof:

Existence: Consider $a + m\underset{\text{unknown}}{t} \equiv b \pmod{n}$.

$$mt \equiv b-a \pmod{n}$$

Solution t exists since $\gcd(m,n)=1$. [Mult. by m is a bijection $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$]

Then $x = a+tm$ works:

$$x = a+tm \equiv a \pmod{m}$$
$$x = a+tm \equiv b \pmod{n}.$$

Uniqueness: Suppose x,y both solve $*$.

Then $z = x-y$ solves: $z \equiv 0 \pmod{m}$, $z \equiv 0 \pmod{n}$

so $m \mid z$ and $n \mid z$ hence $mn \mid z$, so $x \equiv y \pmod{mn}$. $\square$

Application: $\varphi(nm) = \varphi(n)\cdot\varphi(m)$, when $\gcd(n,m)=1$.

Proof: (sketch) $\varphi(nm) = \#(\mathbb{Z}/nm\mathbb{Z})^*$, $\varphi(n)\cdot\varphi(m) = \#(\mathbb{Z}/n\mathbb{Z})^* \cdot \#(\mathbb{Z}/m\mathbb{Z})^*$

(See §2.2.1 of book for details)

$$\mathbb{Z}/nm\mathbb{Z} \xrightarrow[\text{by CRT}]{\cong} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

What's next for algorithms:

Algorithms!

(1) Given $\boxed{ax \equiv b \pmod{n}}$ with $\gcd(a,n)=1$ algorithm to quickly compute solution x. // make explicit CRT easy.

(2) Algorithm to compute powers $x^m \equiv \pmod{n}$ quickly. // Core idea in public-key crypto; primality testing; etc.

Examples.

(sage worksheet)