ACOL 202 Lecture 17

Theorem Let n and m be any two relatively prime integers. For any $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$, there exist one and only one integer $x \in \mathbb{Z}_{nm}$ such that $x \bmod n = a$ and $x \bmod m = b$.

Only one

Suppose not: Let x and x' be such that . . . .

$$x \bmod n = a = x' \bmod n$$
$$x \bmod m = b = x' \bmod m$$

$$x - x' \bmod n = 0 \Rightarrow n \mid x - x'$$
$$x - x' \bmod m = 0 \Rightarrow m \mid x - x'$$

Claim: If n and m are relatively prime, and $n \mid a$ and $m \mid a$ then $nm \mid a$.

$$\Rightarrow nm \mid x - x' \Rightarrow x = x'.$$

Proof of the claims

$n | a \qquad m | a$

$\Rightarrow \quad a = nk_1 \qquad a = mk_2$

$ma = \underline{mnk_1} \qquad na = nmk_2$

$1 = xn + ym$

$a = x\underline{na} + y\underline{ma}$

$xnmk_2 + y\, mnk_1$

$= nm(xk_2 + yk_1)$

Proof that there exist one such x.

n, m are relatively prime.

Extended-Euclid $(n, m) = (c, d, 1)$

$cn + dm = 1 \Rightarrow acn + adm = a$

Claim

$$\boxed{x = (adm + bcn) \bmod nm}$$

We need to prove that $x \bmod n = a$

$x \bmod m = b$

$$((adm + bcn) \bmod nm) \bmod n$$

$$= (adm + bcn) \bmod n \quad [\text{Tutorial 7 Q1}]$$

$$= (adm + 0) \bmod n$$

$$= (adm + acn) \bmod n$$

$$= a \bmod n = a.$$

Proved

Exercise Find $x \in \mathbb{Z}_{30}$

such that $x \bmod 5 = 4$

and $x \bmod 6 = 5$

$n = 5$ $a = 4$ $c = -1$

$m = 6$ $b = 5$ $d = 1$

$(adm + bcn) \bmod nm$

$24 + (-25) \bmod 30$

$= -1 \bmod 30 = 29$

Exercise Find x such that $x \bmod 7 = 1$ and $x \bmod 3 = 5$

$x \bmod 2 = 0$ $\quad$ $x \bmod 3 = 2$ $\quad$ $x \bmod 5 = 1$

$n \quad a \qquad m \quad b$

$\text{Extended-Euclid}(2,3) = (\overset{c}{-1}, \overset{d}{1}, 1)$

$y = (adm + bcn) \bmod nm$

$= -4 \bmod 6$

$= 2$

$c = -1$

$d = 1$

$(6 + 2 \cdot -1 \cdot 5) \bmod 30$

$= -4 \bmod 30$

$= 26.$

$x \bmod \overset{m}{6} = \overset{b}{2}$ $\qquad$ $x \bmod \overset{n}{5} = \overset{a}{1}$

General version
(k congruences)

Let $n_1, n_2, \ldots, n_k$ be integers that are pairwise relatively prime, for some $k \geq 1$. Let $N = \prod_{i=1}^{k} n_i$.

Then for any $\langle a_1 \ldots a_k \rangle$ such that $a_i \in \mathbb{Z}_{n_i}$, there exists one and only one integer $x \in \mathbb{Z}_N$ such that $x \bmod n_i = a_i$ for all i.

Arithmetic over $\mathbb{Z}_n$.

Division

$$\mathbb{Z}_9 = \{0, 1, 2, \dots, 8\}$$

half of 6 ? $= 3$ $\quad 3 \times 2 = 6$

8 ? $= 4$ $\quad 4 \times 2 = 8$

3 ? $= 6$ $\quad 6 \times 2 = 3$

$\underline{7} \times 2 = 5$

0	1	2	3	4	5	6	7	8
0	5	1	6	2	7	3	8	4

Multiplicative identity and inverse (in $\mathbb{R}$)

1 $\quad x \cdot 1 = 1 \cdot x = x$

inverse Not Defined when $x = 0$

in every other case $\frac{1}{x}$.

Multiplicative inverses in $\mathbb{Z}_n$.

$a \in \mathbb{Z}_n$, is $a^{-1} \in \mathbb{Z}_n$

$$a a^{-1} = a^{-1} a = 1$$

If there is no such a^{-1} in $\mathbb{Z}_n$, then not defined.

Multiplicative inverse of 2 in $\mathbb{Z}_9$ $\quad 5$

3 in $\mathbb{Z}_9$ $\quad$ not defined

<u>Claim</u> Let $n \geq 2$ and $a \in \mathbb{Z}_n$

Then a^{-1} exists in $\mathbb{Z}_n$ iff n and a are <u>relatively</u> prime.

$$ax \bmod n = 1$$
$$ay \bmod n = 1$$

$$(ax - ay) \bmod n = 0$$

$$a(x-y) \bmod n = 0$$

$$ax(x-y) \equiv_n 0$$

There cannot be two multiplicative inverses of a in $\mathbb{Z}_n$.

Proof of the claim

By def^n, multiplicative inverse of a exists in $\mathbb{Z}_n$ precisely when there is an integer x such that

$$ax \equiv_n 1.$$

Claim For any $n \geq 2$ and $a \in \mathbb{Z}_n$ there exists $x \in \mathbb{Z}$ with $ax \equiv_n 1$ iff $\exists y \in \mathbb{Z}_n$ st $ay \equiv_n 1$.

We'll prove the claim later.

$$ax \equiv_n 1$$

iff $\quad ax = kn + 1$

iff $\quad ax - kn = 1$

iff $\quad ax + (-k)n = 1$

iff $\quad ax + yn = 1$

There exists a^{-1} in $\mathbb{Z}_n$ iff there exist integers x and y such that $ax + yn = 1$.

a^{-1} exists in $\mathbb{Z}_n$ $\Rightarrow$ a and n are relatively prime.

(Prove the Contrapositive)

a and n not relatively prime

$\gcd(a, n) = d \ (>1)$

$d \mid a \qquad d \mid n$

$a = k_1 d \qquad n = k_2 d$

$ax = \cancel{x}\ x k_1 d$

$yn = y k_2 d$

$ax + yn = d(xk_1 + yk_2)$

$\therefore$ a^{-1} does not exist in $\mathbb{Z}_n$.

Made with Goodnotes

The other direction follows from Extended-Euclid (a, n) which gives $(x, y, 1)$ such that $ax + yn = 1$.

Proof of the claim

One direction — trivial.

$x \in \mathbb{Z}$ $\quad ax \bmod n = 1$.

$y = (x \bmod n)$

$$ay \bmod n = [a(x \bmod n)] \bmod n$$

$$= \left[a\left(x - \left\lfloor \frac{x}{n} \right\rfloor n\right)\right] \bmod n$$

$$= \left(ax - a\left\lfloor \frac{x}{n} \right\rfloor n\right) \bmod n$$

```
inverse (a, n)
    x, y, d = Extended-Euclid (a, n)
    if d = 1
        return x mod n
    else
        return "a^-1 does not exist"
```

Corollary If p is prime then every non-zero $a \in \mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$.

Lemma For any prime p and any non-zero $a \in \mathbb{Z}_p$ the first $(p-1)$ non-zero multiples of a $\underline{\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}}$ is precisely the set $\{1, \ldots, (p-1)\}$

Consider $p = 7$

i	1	2	3	4	5	6
$4i \bmod 7$	4	1	5	2	6	3
$5i \bmod 7$	5	3	1	6	4	2

$ia \bmod p$

$p \nmid ia$

$i \in \{1 \ldots p-1\}$

$a \in \{1 \ldots p-1\}$

Fermat's Little Theorem

Let p be a prime and let $a \in \mathbb{Z}_p$ where $a \neq 0$.

Then $a^{p-1} \equiv_p 1$.

561