Modular arithmetic continued

$a \equiv b \pmod{n}$

$\Leftrightarrow a = b + kn \quad (k \in \mathbb{Z})$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

We could write $[a]_{\equiv n}$ instead of a

How do calculation work?
Use the regular +,−,*,/ from $\mathbb{Z}$, "up to equivalence"

Thm: $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

then:

① $a + c \equiv b + d \pmod{n}$

② $a \cdot c \equiv b \cdot d \pmod{n}$

This says that $\equiv_n$ is more than an equivalence, it's a congruence

Proof: Assume $\exists k, l \in \mathbb{Z}$

$a = b + kn$ and $c = d + ln$

① $a + c = (b + kn) + (d + ln)$
$= (b + d) + \underbrace{(k + l)}_{\in \mathbb{Z}} n$

$\Rightarrow a + c \equiv b + d \pmod{n}$

② $ac = (b + kn)(d + ln)$
$= bd + bln + kdn + kln^2$
$= bd + n \underbrace{(bl + kd + kln)}_{\in \mathbb{Z}}$

$\Rightarrow ab \equiv bd \pmod{n}$

$\square$

Ex: Find remainder of

$$(23^3 \cdot 12^2 + 771) \div 7$$

$$771 = 770 + 1 = 7 \cdot (110) + 1$$

$$\Rightarrow 771 \equiv 1 \pmod 7$$

$$12 = 7 + 5 \Rightarrow 12 \equiv 5 \pmod 7$$

$$23 = 21 + 2 \Rightarrow 23 \equiv 2 \pmod 7$$

Exponents are repeated multiplications

$$\begin{aligned} 23^3 + 12^2 + 771 &\equiv 2^3 \times 5^2 + 1 \pmod 7 \\ &\equiv 8 \times 25 + 1 \pmod 7 \\ &\equiv 1 \times 4 + 1 \pmod 7 \\ &\equiv 5 \pmod 7 \end{aligned}$$

$\boxed{\text{Answer: } 5}$

In order to do arithmetic mod n, you only need to know how to add/multiply numbers between 0 and n-1 (mod n)

Table of operations:
ex: multiplications of mod 4

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ex: mod 2

+	0	1
0	0	1
1	1	0

1 = T
0 = F

XOR

$\cdot$	0	1
0	0	0
1	0	1

AND

$\Rightarrow p \wedge (q \oplus r)$

$\quad = (p \wedge q) \oplus (p \wedge r)$

Subtraction also works

$a - b = a + (-b)$

exponentiation

$a \equiv b \pmod{n} \Rightarrow a^n \equiv b^n$ (Repeated multiplications)

$C^a \equiv C^b \pmod{n}$ does not work!

Ex: $0 \equiv 3 \pmod{3}$

but $2^c = 1$

$2^3 = 8 \equiv 2 \pmod{3}$

New operation: inversion

Ex: In $\mathbb{Z}$ $\quad 2^{1} = \frac{1}{2} \notin \mathbb{Z}$

"Division" or "multiplicative inversion" as in $\mathbb{R}$, is not an operation of $\mathbb{Z}$, (except for 1 and -1). In $\mathbb{Z}_n$, more numbers than ± 1 may be invertible!

Def: b is inverse of $a \pmod{n}$

if $ab \equiv ba \equiv 1 \pmod{n}$

Ex: $2 \cdot 4 = 8 \equiv 1 \pmod{7}$

4 is inverse of 2, and 2 is inverse of 4

Of course, not all numbers are invertible

Ex: mod 4, 2 does not have an inverse

Because
$$\begin{aligned} 0 \times 2 &= 0 \\ 1 \times 2 &= 2 \\ 2 \times 2 &= 0 \\ 3 \times 2 &= 2 \end{aligned}$$

never 1

Thm: if a has an inverse, then that inverse is unique (mod n)

Proof: Let b and c be two inverses of a

$$ab \equiv ba \equiv 1 \pmod{n}$$
$$ac \equiv ca \equiv 1 \pmod{n}$$

Goal: $b \equiv c \pmod{n}$

$$\begin{aligned} b \equiv b\underline{1} &\equiv b(ac) \\ &\equiv (ba)c \\ &\equiv \underline{1}\, c \\ &\equiv c \quad \pmod{n} \end{aligned}$$

Therefore, we can talk about the inverse of a, denoted: a^{-1}

Properties of inverses

① $(a^{-1})^{-1} \equiv a \pmod{n}$

② $(ab)^{-1} \equiv b^{-1}a^{-1} \equiv a^{-1}b^{-1} \pmod{n}$

Proof:

① $(a^{-1})a \equiv a(a^{-1}) \equiv 1 \pmod{n}$

② $(ab)(b^{-1}a^{-1}) \equiv a(bb^{-1})a^{-1} \equiv a\,1\,a^{-1}$
$\equiv a a^{-1} \equiv 1 \pmod{n}$ □

How do we know when the inverse exists, and when it does, how do we calculate it?

Thm: a has an inverse mod n $\iff \gcd(a, n) = 1$

The proof of that them is constructive: it tells us exactly how to find the inverse

$\boxed{\Rightarrow}$ Assume a^{-1} exists

Let $b = a^{-1}$

$\Rightarrow ba \equiv 1 \pmod{n}$

$\Rightarrow ba = 1 + kn$

$\Rightarrow 1 = -kn + ba \Rightarrow \gcd(a, n) = 1$

$\boxed{\Leftarrow}$ Assume $\gcd(a, n) = 1$

Bezout $\Rightarrow 1 = sa + tn$

$sa = 1 - tn$

$sa = 1 \pmod{n}$

$\Rightarrow s \equiv a^{-1} \pmod{n}$

Conclusion: a^{-1} is the Bezout coefficient of a.
we can find it by rolling Euclid's algorithm backward

Ex: find $17^{-1} \pmod{20}$

Let's find $\gcd(17, 20)$

$20 = 1 \cdot 17 + 3$

$17 = 5 \times 3 + 2$

$3 = 1 \times 2 + \boxed{1}$ gcd $\Rightarrow 17^{-1}$ exists

$2 = 2 \times 1 + 0$

Rollback:

$$1 = 3 - 1 \times 2$$
$$= 3 - 1(17 - 5 \times 3)$$
$$= 6 \times 3 - 1 \times 17$$
$$= 6(20 - 1 \times 17) - 1 \times 17$$
$$= 6 \times 20 - 7 \cdot 17 \Rightarrow 17^{-1} \equiv -7 \pmod{20}$$
$$\equiv 13 \pmod{20}$$

Ex: solve $7x + 18 \equiv 13 \pmod{20}$

$$7x \equiv 13 - 18 \pmod{20}$$
$$7^{-1}(7x) \equiv (-5)\,7^{-1} \pmod{20}$$
$$x \equiv (-5)\,7^{-1} \; (?)$$

We know $17^{-1} \equiv -7 \pmod{20}$

$$(-17^{-1}) \equiv 7 \pmod{20}$$
$$\Rightarrow 7^{-1} \equiv ((-17)^{-1})^{-1} \pmod{20}$$
$$7^{-1} \equiv -17 \pmod{20}$$

That means $x \equiv (-5)(-17)$

$$\equiv (-5)(3)$$
$$\equiv -15 \equiv 5 \pmod{20}$$

Prime modular arithmetic (mod p (where p is prime))

Lemma: $\forall a \in \mathbb{Z}$, either $p \mid a$

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

Proof: Assume $p \nmid a$, then if $d = \gcd(a, p)$

then $d = 1$ or $d = p$ Impossible

$\square$

Consequence: either $a \equiv 0 \pmod p$
or a is invertible $\pmod p$

$\Rightarrow$ All numbers except 0 is invertible (mod p)

In algebra, we would say that $\mathbb{Z}_p$ is a field
(like $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \ldots$)

Thm (integrity):

$$ab \equiv 0 \pmod p \Rightarrow a \equiv 0 \pmod p$$
$$\text{or } b \equiv 0 \pmod p$$

*Note: This is not true in general

Ex: mod 6 (not prime

$$2 \times 3 = 6 \equiv 0 \pmod 6$$

But $2 \not\equiv 0$ and $3 \not\equiv 0 \pmod 6$

Proof (prime p)

Assume $ab \equiv 0 \pmod p$

Assume $a \not\equiv 0 \pmod p \Rightarrow a^{-1}$ exists

$$\Rightarrow a^{-1} ab \equiv a^{-1} 0 \pmod p$$
$$b \equiv 0 \pmod p$$

$\square$

Ex: Solve $x^2 \equiv x \pmod 7$

$$x^2 - x \equiv 0 \pmod 7$$
$$x(x-1) \equiv 0 \pmod 7$$

By integrity: $\boxed{x \equiv 0}$ or $x - 1 \equiv 0 \pmod 7$

$$\boxed{x \equiv 1} \pmod 7$$

Actually, for (mod 6), there are more solutions, like x=3

check: $3^2 = 9 \equiv 3 \pmod{6}$