Defn

$a \underline{\text{mod}}\ m = r$ s.t. $0 \le r < m$ and $a = qm + r$

function $\mathbb{Z} : \{0 \ldots m-1\}$

Defn $a \equiv b \pmod{m}$

relation

$m \mid (a-b)$

$a = b + \cdot Km$ for some K

Thm $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$

Then $a + c \equiv b + d \pmod{m}$

$ac \equiv bd \pmod{m}$

$m \mid a-b$

$m \mid c-d$

$\therefore m \mid (a-b)+(c-d)$

$\therefore m \mid =(a+c)-(b+d)$

$\therefore a+c \equiv b+d \pmod{m}$

if $ac \equiv bc \pmod{m}$

is $a \equiv b \pmod{m}$?

$14 \equiv 8 \pmod{6}$

$7 \not\equiv 4 \pmod{6}$

but always true if $\gcd(m,c)=1$

<u>pf</u> $m \mid ac - bc$

$m \mid c(a-b)$

since $\gcd(m,c)=1$

$\therefore m \mid a-b$

$\therefore a \equiv b \bmod m$

when/how solve

$$ax \equiv b \pmod{m}$$

if I had $\bar{a}$ st $\bar{a} \cdot a \equiv 1 \pmod{m}$

Thm if $\gcd(a, m) = 1$

then $\exists\ \bar{a}$ st $a\bar{a} \equiv 1 \pmod{m}$

[multiplicative inverse of a]

[Furthermore $\bar{a}$ is unique up to mod m]

proof (existence only)

$\exists\ s, t$ st $s \cdot a + t \cdot m = 1$

$$tm \equiv 0 \pmod{m}$$

$$-tm \equiv 0 \pmod{m}$$

$$\begin{array}{rl} sa + tm \equiv 1 & \pmod{m} \\ -tm \equiv 0 & \pmod{m} \\ \hline sa \equiv 1 & \pmod{m} \end{array}$$

(can find $\bar{a} = s$ via Euclid)

Chinese Remainder Theorem (CRT)

$x \equiv a_i \pmod{m_i}$ for $i = 1, 2 \ldots n$

$\gcd(m_i, m_j) = 1$ for $i \neq j$

$\exists$ unique $0 \leq x < M = \prod m_i$
satisfying these equations.

Proof

let $M_k = M / m_k$

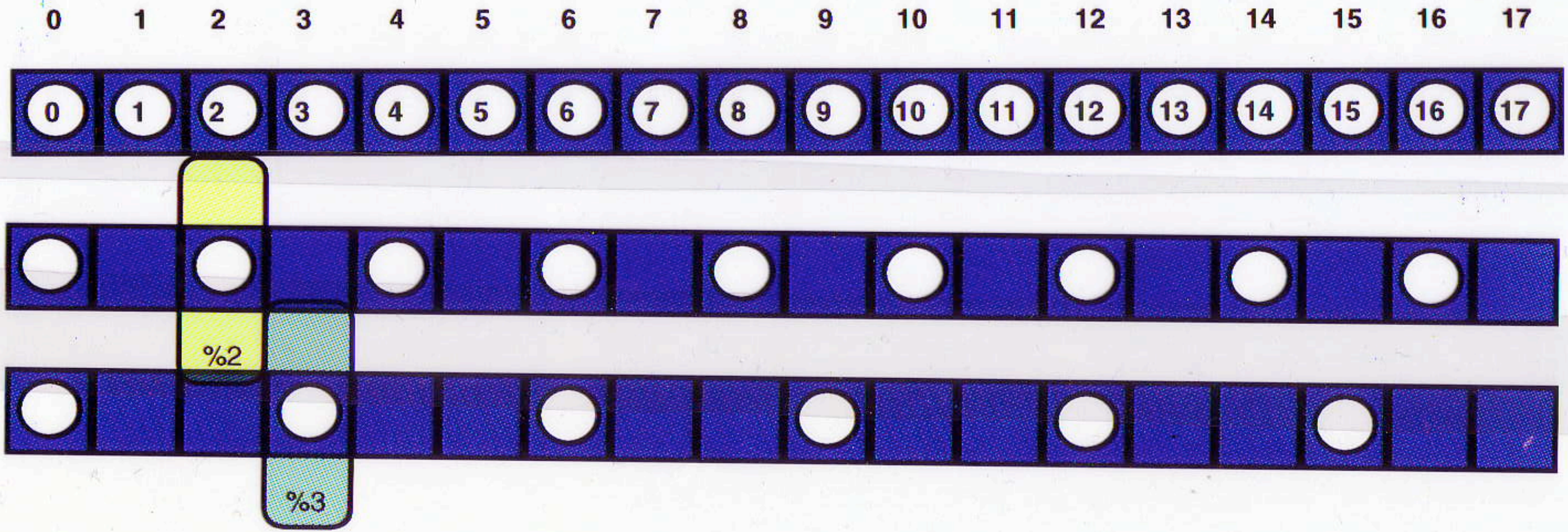
$y_k \cdot M_k \equiv 1 \pmod{m_k}$

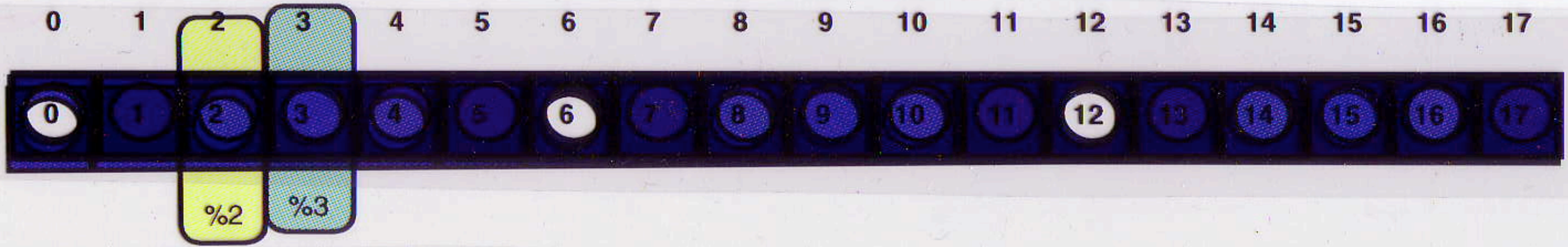
$\exists$ since $\gcd(M_k, m_k) = 1$

$$x = \underbrace{\sum_i a_i M_i y_i}_{(\text{mod } m_j)}$$

$$\equiv a_j M_j y_j \pmod{m_j}$$

$$\equiv a_j \pmod{m_j}$$


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
%2
%3


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
%2
%3

Fermat's Little Theorem

if p is prime $p \nmid a$

Then $a^{p-1} \equiv 1 \pmod p$

$[\forall a \quad a^p \equiv a \pmod p]$

$a^i \bmod n$ for $a=5$, $n=10$

$5 \quad 25 \bmod 10 = 5$

$5^3 = 125 \bmod 10 = 5$

$\vdots$

$5^9 \equiv 5 \bmod 10$

---

fact $2^{n-1} \not\equiv 1 \pmod n$

for all but 22 composite numbers $n < 10\,000$

Fermat's Little Theorem

If p is prime and $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p}$$

And for all a

$$a^p \equiv a \pmod{p}$$

See also Rosen 3.7 #17

Proof

$\gcd(a, p) = 1$

$f: Z_p \to Z_p \quad f(i) = a\,i \bmod p$ is bijection

$\left[\; i a \equiv j a \pmod{p} \Rightarrow i \equiv j \pmod{p} \;\right]$

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} f(i)$$

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

$$\gcd((p-1)!, p) = 1$$

$$1 \equiv a^{p-1} \pmod{p}$$

RSA - A Public Key Cryptosystem

Alice:

① <u>Privately</u> chooses two primes p, q of, say, 500 bits each, and an e rel. prime to $(p-1)(q-1)$.

② <u>Privately</u> computes $n = p \cdot q$ and d such that $ed \equiv 1 (\mathrm{mod}\ (p-1)\cdot(q-1))$

③ <u>Publishes</u> n and e in the phone book
(Keep p, q, d <u>private</u>.)

Bob (or anyone else):

Sends her an encrypted message M by looking up her n, e and sending $c = M^e \ \underline{\mathrm{mod}}\ n$

Alice decrypts by computing

$$c^d \ \underline{\mathrm{mod}}\ n = M.$$

Issues:
- do e, d always exist?
- how hard to compute?
- why $(M^e)^d \bmod n = M$?
- how [illegible]?