For any feild F

Notation

$$\mathrm{char}(F) = \text{least } n \text{ s.t. } \underset{\underbrace{1+1+\cdots+1}_{n \text{ times}}}{\overset{\|}{n\cdot 1}} = 0 \text{ in } F$$

$a \cdot 1 = a$

$= 1 \cdot a \quad = n \cdot (1a)$

$= (n\cdot 1)\, a$

$\uparrow$ $= 0$

Lemma: Let $m, n \in \mathbb{Z}$ $m, n \geq 0$ $\gcd(m,n) = 1$

For $a, b \in \mathbb{Z}$ the system

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

has a solution. If x_1, x_2 are solutions

$$x_1 \equiv x_2 \pmod{mn}.$$

Proof:

$x \equiv a \pmod m$ has a solution

$x = a + km \quad \forall k \in \mathbb{Z}$

Show $\exists$ $k_1 \in \mathbb{Z}$ s.t. $a + k_1 m \equiv b \mod \underline{n}$

$\Leftarrow$ Show $k \cdot m \equiv b-a \mod n$

Since $\gcd(m,n)=1 \Rightarrow \exists\, s,t \in \mathbb{Z}$ s.t.

$$ms + nt = 1$$

$$ms = 1 - nt$$

$$(b-a)ms = (b-a) - (b-a)nt$$

$$\underbrace{((b-a)s)}_{k_1} m \equiv b-a \mod n$$

$\therefore$ $k_1 = (b-a)s$ is a solution

c_1, c_2 s.t.

$$c_1 \equiv c_2 \equiv a \mod m$$

$$c_1 \equiv c_2 \equiv b \mod n$$

$$c_1 \equiv c_2 \mod m$$

$$c_1 \equiv c_2 \mod n$$

$\therefore$ m, n divide $c_1 - c_2$

m n in here, m in here

$$c_1 - c_2 = k_1 m = k_2 n \qquad (\text{since } \gcd(m,n)=1)$$

$$\Rightarrow \quad c_1 - c_2 = \hat{k}\, mn$$

$$\Rightarrow \quad c_1 \equiv c_2 \mod mn$$

∎

Chinese Remainder Theorem

Let $n_1, \dots, n_k$ be positive integers s.t. $\gcd(n_i, n_j) = 1$ $\forall\, i \neq j$
for any $a_1, \dots, a_k$

$$x = a_1 \mod n_1$$
$$x = a_2 \mod n_2$$
$$\vdots$$
$$x = a_k \mod n_k$$

has a solution. Further any two sol. are equal mod $n_1 \cdots n_k$.

Proof: Induction + Lemma.

Example:

$$\left.\begin{aligned} x &= 3 \mod 4 \\ x &= 4 \mod 5 \end{aligned}\right\} \; x = 19 \qquad x = 19 \mod 20$$
$$x = 1 \mod 9$$
$$x = 5 \mod 7$$

19 is also a sol

$$x = 19 \mod 180$$
$$x = 5 \mod 7$$

$$x = 19 \mod 1260.$$