

3.4 Chinese remainder theorem

Example 81. (warmup)

- (a) If $x \equiv 3 \pmod{10}$, what can we say about $x \pmod{5}$?
- (b) If $x \equiv 3 \pmod{7}$, what can we say about $x \pmod{5}$?

Solution.

- (a) If $x \equiv 3 \pmod{10}$, then $x \equiv 3 \pmod{5}$.
[Why?! Because $x \equiv 3 \pmod{10}$ if and only if $x = 3 + 10m$, which modulo 5 reduces to $x \equiv 3 \pmod{5}$.]
- (b) Absolutely nothing! $x = 3 + 7m$ can be anything modulo 5 (because $7 \equiv 2$ is invertible modulo 5).

Example 82. If $x \equiv 32 \pmod{35}$, then $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Why?! As in the first part of the warmup, if $x \equiv 32 \pmod{35}$, then $x \equiv 32 \pmod{5}$ and $x \equiv 32 \pmod{7}$.

The Chinese remainder theorem says that this can be reversed!

That is, if $x \equiv 2 \pmod{5}$ and $x \equiv 4 \pmod{7}$, then the value of x modulo $5 \cdot 7 = 35$ is determined.

[How to find the exact $x \equiv 32 \pmod{35}$ is discussed in the next example.]

Theorem 83. (Chinese Remainder Theorem) Let n_1, n_2, \dots, n_r be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad \dots, \quad x \equiv a_n \pmod{n_r}$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$.

In other words. The Chinese remainder theorem provides a bijective (i.e., 1-1 and onto) correspondence

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod{n} \\ x \pmod{m} \end{bmatrix}.$$

For instance. Let's make the correspondence explicit for $n = 2$, $m = 3$:

$$0 \mapsto \begin{bmatrix} 0 \\ 0 \end{bmatrix}, 1 \mapsto \begin{bmatrix} 1 \\ 1 \end{bmatrix}, 2 \mapsto \begin{bmatrix} 0 \\ 2 \end{bmatrix}, 3 \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}, 4 \mapsto \begin{bmatrix} 0 \\ 1 \end{bmatrix}, 5 \mapsto \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

Example 84. Solve $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Solution. $x \equiv 2 \cdot 7 \cdot \underbrace{7^{-1}_{\pmod{5}}}_3 + 4 \cdot 5 \cdot \underbrace{5^{-1}_{\pmod{7}}}_3 = 42 + 60 \equiv 32 \pmod{35}$

Important comment. Can you see how we really need 5 and 7 to be coprime here?

Brute force solution. Note that, while in principle we can always perform a brute force search, this is not practical for larger problems. Here, if x is a solution, then so is $x + 35$. So we only look for solutions modulo 35.

Since $x \equiv 4 \pmod{7}$, the only candidates for solutions are 4, 11, 18, ... Among these, we find $x = 32$.

[We can also focus on $x \equiv 2 \pmod{5}$ and consider the candidates 2, 7, 12, ..., but that is even more work.]

Example 85. Solve $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.

Solution. $x \equiv 1 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)_{\pmod{4}}^{-1}]_3} + 2 \cdot 4 \cdot 7 \cdot \underbrace{[(4 \cdot 7)_{\pmod{5}}^{-1}]_2} + 3 \cdot 4 \cdot 5 \cdot \underbrace{[(4 \cdot 5)_{\pmod{7}}^{-1}]_{-1}} = 105 + 112 - 60 = 157 \equiv 17 \pmod{140}$.

Example 86. (homework)

- (a) Solve $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{25}$.
- (b) Solve $x \equiv -1 \pmod{4}$, $x \equiv 2 \pmod{7}$, $x \equiv 0 \pmod{9}$.

Solution. (final answer only)

- (a) $x \equiv 78 \pmod{100}$
- (b) $x \equiv 135 \pmod{252}$

Silicon slave labor. For the second part of this problem check out the following command in Sage:

```
Sage] crt([-1,2,0], [4,7,9])
135
```

Example 87.

- (a) Let $p > 3$ be a prime. Show that $x^2 \equiv 9 \pmod{p}$ has exactly two solutions (i.e. ± 3).
- (b) Let $p, q > 3$ be distinct primes. Show that $x^2 \equiv 9 \pmod{pq}$ always has exactly four solutions (± 3 and two more solutions $\pm a$).

Solution.

- (a) If $x^2 \equiv 9 \pmod{p}$, then $0 \equiv x^2 - 9 = (x - 3)(x + 3) \pmod{p}$. Since p is a prime it follows that $x - 3 \equiv 0 \pmod{p}$ or $x + 3 \equiv 0 \pmod{p}$. That is, $x \equiv \pm 3 \pmod{p}$.
- (b) By the CRT, we have $x^2 \equiv 9 \pmod{pq}$ if and only if $x^2 \equiv 9 \pmod{p}$ and $x^2 \equiv 9 \pmod{q}$. Hence, $x \equiv \pm 3 \pmod{p}$ and $x \equiv \pm 3 \pmod{q}$. These combine in four different ways. For instance, $x \equiv 3 \pmod{p}$ and $x \equiv 3 \pmod{q}$ combine to $x \equiv 3 \pmod{pq}$. However, $x \equiv 3 \pmod{p}$ and $x \equiv -3 \pmod{q}$ combines something modulo pq which is different from 3 or -3 .

Why primes > 3 ? Why did we exclude the primes 2 and 3 in this discussion?**Comment.** There is nothing special about 9 . The same is true for $x^2 \equiv a^2 \pmod{pq}$ any integer a .**Example 88. (homework)** Let m, n be coprime. Show that a is a quadratic residue modulo mn if and only if a is a quadratic residue modulo both m and n .**Solution.** a is a quadratic residue modulo mn

$$\iff a \equiv x^2 \pmod{mn} \text{ (for some integer } x)$$

$$\iff [\dots \text{ apply CRT } \dots]$$

Example 89. (homework) Determine all solutions to $x^2 \equiv 9 \pmod{35}$.**Solution. (final answer only)** The solutions are $x \equiv \pm 3 \pmod{35}$ and $x \equiv \pm 17 \pmod{35}$.**Silicon slave labor.** Again, we can let Sage do the work for us:

```
Sage] solve_mod(x^2 == 9, 35)
[(17), (32), (3), (18)]
```