Theorem 66. (Chinese Remainder Theorem) Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

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

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

$$x \pmod{nm} \mapsto \left[\begin{array}{c} x \pmod{n} \\ x \pmod{m} \end{array}\right].$$

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

$0 \mapsto \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $1 \mapsto \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$, $2 \mapsto \left[\begin{smallmatrix} 0 \\ 2 \end{smallmatrix}\right]$, $3 \mapsto \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $4 \mapsto \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$, $5 \mapsto \left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$

Example 67. Solve $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.

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

Silicon slave labor. Once you are comfortable doing it by hand, you can easily let Sage do the work for you:

```
Sage] crt([1,2,3], [4,5,7])
```

17

Example 68. (extra)

(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) $x \equiv 135 \pmod{252}$

Example 69.

(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 $x \equiv -3 \pmod{q}$ combine to 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 $x^2 \equiv a^2 \pmod{pq}$ for any integer a.

Armin Straub
straub@southalabama.edu

Example 70. Determine all solutions to $x^2 \equiv 9 \pmod{35}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 9 \pmod{35} \\ \iff & x^2 \equiv 9 \pmod{5} \text{ and } x^2 \equiv 9 \pmod{7} \\ \iff & x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{7} \end{aligned}$$

The two obvious solutions modulo 35 are ± 3. To get one of the two additional solutions, we solve $x \equiv 3 \pmod{5}$, $x \equiv -3 \pmod{7}$. [Then the other additional solution is the negative of that.]

$$x \equiv 3 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 5}}_{3} - 3 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 7}}_{3} \equiv 63 - 45 \equiv 18 \pmod{35}$$

Hence, the solutions are $x \equiv \pm 3 \pmod{35}$ and $x \equiv \pm 18 \pmod{35}$. [$\pm 18 \equiv \pm 17 \pmod{35}$]

Silicon slave labor. Again, we can let Sage do the work for us:

```
Sage] solve_mod(x^2 == 9, 35)
```

$[(17), (32), (3), (18)]$

Review: quadratic residues

Definition 71. An integer a is a **quadratic residue** modulo n if $a \equiv x^2 \pmod{n}$ for some x.

Example 72. List all quadratic residues modulo 11.

Solution. We compute all squares: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 5$, $(\pm 5)^2 \equiv 3$. Hence, the quadratic residues modulo 11 are $0, 1, 3, 4, 5, 9$.

Important comment. Exactly half of the 10 nonzero residues are quadratic. Can you explain why?

[*Hint.* $x^2 \equiv y^2 \pmod{p} \iff (x-y)(x+y) \equiv 0 \pmod{p} \iff x \equiv y$ or $x \equiv -y \pmod{p}$]

Example 73. List all quadratic residues modulo 15.

Solution. We compute all squares modulo 15: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 1$, $(\pm 5)^2 \equiv 10$, $(\pm 6)^2 \equiv 6$, $(\pm 7)^2 \equiv 4$. Hence, the quadratic residues modulo 15 are $0, 1, 4, 6, 9, 10$.

Important comment. Among the $\phi(15) = 8$ invertible residues, the quadratic ones are $1, 4$ (exactly a quarter). Note that 15 is of the form $n = pq$ with p, q distinct primes. Example 75 explains why this always happens for such n.

Example 74. 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

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

$\iff$ $a \equiv x^2 \pmod{m}$ and $a \equiv x^2 \pmod{n}$ (for some integer x)

$\iff$ a is a quadratic residue modulo both m and n

It is obvious that "$\Longrightarrow$" holds in the final step. To see that "$\Longleftarrow$" also holds is a bit more tricky: if $a \equiv x^2 \pmod{m}$ and $a \equiv y^2 \pmod{n}$, then we can find s, t such that $x - y = sm + tn$ (possible by Bezout because m, n are coprime) or, equivalently, $x - sm = y + tn$. Then, with $X = x - sm$, we have $a \equiv X^2 \pmod{m}$ and $a \equiv X^2 \pmod{n}$.

Example 75. Show why, if $n = pq$ with p, q distinct primes, exactly a quarter of all invertible residues modulo n are quadratic.

Solution. As we saw in the previous example, a is a quadratic residue modulo $n = pq$ if and only if a is a quadratic residue both modulo p and modulo q. We have $\phi(p)/2$ invertible quadratic residues modulo p, and $\phi(q)/2$ invertible quadratic residues modulo q. These combine to $\frac{\phi(p)}{2} \cdot \frac{\phi(q)}{2} = \frac{\phi(n)}{4}$ (invertible quadratic) residues modulo $n = pq$.