MODULAR ARITHMETIC III

PETER MCNAMARA

Bucknell University
and Trinity College Dublin

Main definition

$$a \equiv b \pmod{m} \quad \text{if}$$

$$m \mid a - b \quad \text{i.e. } m \text{ divides } a - b.$$

This is equivalent to a and b having the same remainder under division by m.

Motivating Problem.

We know how to find k that satisfies $77^k \equiv 1 \pmod{100}$. How?

Now find k that satisfies $77k \equiv 1 \pmod{100}$.

1. EUCLID'S ALGORITHM

Two problems:

(a) Find $\gcd(153, 442) = d$.

(b) Find r and s such that $r(153) + s(442) = d$.

Euclid's Algorithm, also know as the Euclidean Algorithm, answers both of these questions quickly.

$$442 = 2\,.\,153 + 136 \qquad d = \gcd(153, 136)$$

$$153 = 1\,.\,136 + 17 \qquad d = \gcd(136, 17)$$

$$136 = 8\,.\,17 + 0 \qquad d = \gcd(17, 0) = \boxed{17}$$

Now work backwards to find r and s:

$$\begin{aligned} 17 &= 153 - 1\,.\,136 \\ &= 153 - (442 - 2\,.\,153) \\ &= 3\,.\,153 - 442. \end{aligned}$$

Answer: $\boxed{r = 3 \text{ and } s = -1}$

Problem 1. Find some k so that $77k \equiv 1 \pmod{100}$.

Solution.

Claim. If $\gcd(m, n) = 1$, then there exists r with $rm \equiv 1 \pmod{n}$.

Proof of Claim. By Euclid's Algorithm, $1 = rm + sn$ for some r and s.

Therefore, $rm \equiv 1 - sn \equiv 1 \pmod{n}$, as required.

In seats. Use Euclid's Algorithm on 100 and 77 to solve Problem 1.

$$100 = 1\,.\,77 + 23$$

$$77 = 3\,.\,23 + 8$$

$$23 = 2\,.\,8 + 7$$

$$8 = 1\,.\,7 + 1$$

$$7 = 7\,.\,1 + 0$$

Now work backwards:

$$\begin{aligned} 1 &= 8 - 7 \\ &= 8 - (23 - 2\,.\,8) \\ &= 3\,.\,8 - 23 \\ &= 3(77 - 3\,.\,23) - 23 \\ &= 3\,.\,77 - 10\,.\,23 \\ &= 3\,.\,77 - 10(100 - 77) \\ &= 13\,.\,77 - 10\,.\,100 \end{aligned}$$

Thus

$$13\,.\,77 \equiv 1 + 10\,.\,100 \equiv 1 \pmod{100}.$$

Answer: $\boxed{13}$

Problem 2. Using the result of Problem 1, find $77^{77} \pmod{100}$ in a fancier way than before.

Solution. 2 things we know:

1. $77 \,.\, 13 \equiv 1 \pmod{100}$.

2. $77^{\phi(100)} \equiv 1 \pmod{100}$.

What's $\phi(100)$?

$$\phi(100) = \phi(4\,.\,25) = \phi(2^2 5^2) = (2^2 - 2)(5^2 - 5) = 40.$$

We get

$$\begin{aligned} 77^{40} &\equiv 1 \pmod{100} \\ 77^{80} &\equiv 1 \pmod{100} \\ 13\,.\,77^{80} &\equiv 13 \pmod{100} \\ 13\,.\,77\,.\,77^{79} &\equiv 13 \pmod{100} \\ 1\,.\,77^{79} &\equiv 13 \pmod{100} \end{aligned}$$

Multiply twice more by 13 to wither it down to

$$\begin{aligned} 77^{77} &\equiv 13^3 \pmod{100} \\ &\equiv \boxed{97} \pmod{100}. \end{aligned}$$

2. CHINESE REMAINDER THEOREM

$6, 10, 15$ are coprime since $\gcd(6, 10, 15) = 1$ but they are **not pairwise coprime** since

$\gcd(6, 10) = 2$,

$\gcd(6, 15) = 3$,

$\gcd(10, 15) = 5$.

Chinese Remainder Theorem. Given integers $n_1, n_2, \ldots, n_k$ that are pairwise coprime and any integers $a_1, a_2, \ldots, a_k$, then there exists an integer x such that

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ x &\equiv a_3 \pmod{n_3}, \\ \vdots\ &\ \vdots\ \ \vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

Furthermore, if x' is another solution of this system then

$$x' \equiv x \pmod{n_1 n_2 \cdots n_k}.$$

Proof (as time permits). Since n_1 and n_2 are coprime, we can find r and s such that

$$1 = r\,n_1 + s\,n_2.$$

So

$$s\,n_2 \equiv 1 - r\,n_1 \equiv 1 \pmod{n_1},$$

$$r\,n_1 \equiv 1 - s\,n_2 \equiv 1 \pmod{n_2}.$$

The trick: let $x = a_1\,s\,n_2 + a_2\,r\,n_1$.

$$x \equiv a_1\,s\,n_2 + 0 \equiv a_1 \pmod{n_1},$$

$$x \equiv 0 + a_2\,r\,n_1 \equiv a_2 \pmod{n_2}.$$

Now consider n_3, and use the same technique to find y such that

$$y \equiv a_3 \pmod{n_3},$$

$$y \equiv x \pmod{n_1 n_2},$$

so

$$y \equiv x \equiv a_1 \pmod{n_1},$$

$$y \equiv x \equiv a_2 \pmod{n_2}.$$

And so on...

If x' is another solution, then $x' - x$ is divisible by $n_1, n_2, \ldots, n_k$. Since the n_i have no common factors, $x' - x$ is divisible by $n_1 n_2 \cdots n_k$, i.e.,

$$x' \equiv x \pmod{n_1 n_2 \cdots n_k}.$$

Example. Find the smallest positive integer n such that n leaves a remainder of 10 on division by 33 and n leaves a remainder of 13 on division by 47.

In other words,

$$n \equiv 10 \pmod{33},$$
$$n \equiv 13 \pmod{47}.$$

As before, can work out that

$$1 = 10\,.\,33 - 7\,.\,47.$$

In seats:

$$\begin{aligned} n &= a_1\, s\, n_2 + a_2\, r\, n_1 \\ &= 10\,.\,(-7)\,.\,47 + 13\,.\,10\,.\,33 \\ &= 10(13\,.\,33 - 7\,.\,47) \\ &= 10(429 - 329) \\ &= \boxed{1000}. \end{aligned}$$

Important: is this the smallest solution?

Any other solution x satisfies

$$x \equiv 1000 \pmod{33\,.\,47 = 1551}.$$

Since $0 \leq 1000 < 1551$, it must be that $\boxed{1000}$ is the smallest positive solution.

Problem 3. Find the smallest positive n such that

$$\begin{aligned} n &\equiv 1 \pmod{2}, \\ n &\equiv 2 \pmod{3}, \\ n &\equiv 3 \pmod{4}, \\ n &\equiv 4 \pmod{5}, \\ n &\equiv 5 \pmod{6}, \\ n &\equiv 6 \pmod{7}, \\ n &\equiv 7 \pmod{8}, \\ n &\equiv 8 \pmod{9}, \\ n &\equiv 9 \pmod{10}. \end{aligned}$$

Solution. One solution is -1, except that it is not positive. We know that n must satisfy

$$n \equiv -1 \pmod{n_1 n_2 \cdots n_k}$$

except that $2, 3, \ldots, 10$ are not pairwise relatively prime. Instead consider the system

$$\begin{aligned} n &\equiv 4 \pmod{5}, \\ n &\equiv 6 \pmod{7}, \\ n &\equiv 7 \pmod{8}, \\ n &\equiv 8 \pmod{9}. \end{aligned}$$

We check that every solution of this new system is a solution of the original system, and vice versa. Now we have that our moduli of 5, 7, 8, 9 are pairwise relatively prime. So

$$n \equiv -1 \pmod{5 \,.\, 7 \,.\, 8 \,.\, 9}$$

.

The first positive solution is $n = -1 + 5 \,.\, 7 \,.\, 8 \,.\, 9 = -1 + 2520 = \boxed{2519}$.