# MODULAR ARITHMETIC II

PETER MCNAMARA

Bucknell University
and Trinity College Dublin

**Recap of last time.**

**1.**
$$a \equiv b \pmod{m} \quad \text{if}$$
$$m \mid a - b \qquad \text{i.e. } m \text{ divides } a - b.$$

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

**2.** If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ then
$$a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

**3.** Fermat's Little Theorem: for any prime $p$ and any integer $a$ such that $p \nmid a$ (i.e. $p$ does not divide $a$),
$$a^{p-1} \equiv 1 \pmod{p}.$$

While we made use of Fermat's Little Theorem last time, it has an obvious shortcoming. Thoughts?

We'd like a version that works when $p$ is not prime.

**Motivating Problem.**

Find the last two digits of $77^{77}$.

In other words, what is $77^{77}$ (mod 100)?

## 1. EULER'S TOTIENT THEOREM

**Definition.** The *greatest common divisor* of two integers $a$ and $b$, written $\gcd(a, b)$, is the largest integer that divides both of them. If $\gcd(a, b) = 1$, then we say that $a$ and $b$ are *relatively prime* or *coprime* or that they have *no common factor*.

**Examples.** $\gcd(9, 30) = 3$, while 10 and 21 are relatively prime.

**Euler's Totient Theorem.** For any number $m$ and any integer $a$ that is relatively prime to $m$,

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

where $\phi(m)$ is Euler's totient function, defined as the number of integers between 1 and $m$ inclusive that are relatively prime to $m$.

**Examples.**

(a) **In seats:** What's $\phi(25)$?

$$2^{20} \equiv 1 \pmod{25}.$$

(b) If $p$ is prime, what's $\phi(p)$?

We get: if $a$ is relatively prime to $p$, then

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

This is exactly Fermat's Little Theorem!

**Question coming up:** how do we calculate $\phi(m)$ in general?

**Problem 1.** Find $77^{77} \pmod{100}$.

**Solution.** Strategy: $100 = 4\,.\,25$. Let's calculate $77^{77} \pmod 4$ and $77^{77} \pmod{25}$ and go from there.

**In seats:** Calculate $77^{77} \pmod 4$.

Since $77 \equiv 1 \pmod 4$,

$$77^{77} \equiv 1^{77} \equiv 1 \pmod 4.$$

Next, $77 \equiv 2 \pmod{25}$,

$$77^{77} \equiv 2^{77} \pmod{25}.$$

We know that since $\phi(25) = 20$,

$$2^{20} \equiv 1 \pmod{25}.$$

$$2^{77} \equiv (2^{20})^3 2^{17} \equiv 1^3\,.\,2^{17} \equiv 2^{17} \pmod{25}.$$

Now we just find some reasonably simple way to compute $2^{17} \pmod{25}$.

$$2^5 \equiv 32 \equiv 7 \pmod{25}$$

$$2^{10} \equiv (2^5)^2 \equiv 7^2 \equiv 49 \equiv -1 \pmod{25}.$$

Finally,

$$2^{17} \equiv 2^5\,.\,2^{10}\,.\,2^2 \equiv 7\,.\,(-1)\,.\,4 \equiv -28 \equiv -3 \equiv 22 \pmod{25}.$$

To finish the problem, find a number $< 100$ that's congruent to $1 \pmod 4$ and $22 \pmod{25}$.

22, 47, 72, 97. Answer: $\boxed{97}$

# 2. CALCULATING THE TOTIENT FUNCTION

$$\phi(m) = \{1 \le r \le m \mid \gcd(r, m) = 1\}.$$

- We know $\phi(p) = p - 1$ when $p$ is prime.
- Next, consider $\phi(p^a)$ when $p$ is prime and $a > 1$.

  $r$ and $p^a$ have a common factor if and only if $p$ divides $r$.

  $r = p, 2p, 3p, \ldots, p^a$.

  Thus $\boxed{\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).}$

- **In seats:** Is it true that $\phi(a \,.\, b) = \phi(a)\phi(b)$?

  If not, are there conditions on $a$ and $b$ that make it true?

  If $\gcd(a, b) = 1$, then $\phi(a \,.\, b) = \phi(a)\phi(b)$.

- Every $m$ can be written in the form

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

  where each $p_i$ is prime. So

$$\phi(m) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}).$$

- **Example.** Find a positive number $b$ so that

$$77^b \equiv 1 \pmod{200}.$$

$$b = \phi(200) = \phi(2^3 5^2) = (2^3 - 2^2)(5^2 - 5^1) = \boxed{80}$$

## 3. 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.

$$442 = 2\,.\,153 + 136 \qquad\qquad d = \gcd(153, 136) \quad \text{Why?}$$

$d|153$ and $d|442 \quad \Rightarrow \quad d|(442 - 2\,.\,153) = 136.$ Conversely, $d|153$ and $d|136 \quad \Rightarrow \quad d|442.$

So the pairs $(153, 442)$ and $(153, 136)$ have the same sets of divisors and so the same gcd.

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

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

Now work backwards to find $r$ and $s$:

**************** Got this far on 23rd March *****************

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

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

**Problem 2.** Find $k$ so that $77k \equiv 1 \pmod{100}$.

(Compare with $77^k \equiv 1 \pmod{100}$.)

**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 2.

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

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

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

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

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

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: $\boxed{13}$

For the road...

**Problem 4.** If $a$ and $b$ are relatively prime, Euclid's Algorithm gives us a way to find $r$ and $s$ such that $ra + sb = 1$. Show the converse: if there exist $r$ and $s$ such that $ra + sb = 1$, then $a$ and $b$ are relatively prime.

**Problem 5.** Show that $\gcd(3k + 2, 5k + 3) = 1$ for any integer $k$.

**Problem 6.** Suppose you have a cup of that holds 51 ml and another that holds 23 ml, and a one liter jug. Show that by adding a removing full cups from the jug, there is a way to measure out 500 ml.

**Problem 7.** In Problem 2, we learned that $77 \,.\, 13 \equiv 1 \pmod{100}$. Use this to solve Problem 1 again, this time starting with

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

**Problem 8 (IMO 1978, Q1).** Let $m$ and $n$ be natural numbers with $1 \leq m < n$. In their decimal representations the last 3 digits of $1978^m$ and $1978^n$ are equal. Find $m$ and $n$ such that $m + n$ is as small as possible.