Fermat's little theorem, Chinese Remainder Theorem

25 October

We have repeatedly used the fact that

Lemma 1. *If* $a \equiv x \mod n$ *and* $b \equiv y \mod n$ *then*

$$a + b \equiv x + y \mod n$$
$$ab \equiv xy \mod n.$$

For example, we needed to show that

$$n^5 + 4n \equiv 0 \mod 5.$$

If $n \equiv a \mod 5$ then $n^5 \equiv a^5 \mod 5$ and $4n \equiv 4a \mod 5$, so it is sufficient to consider the residue classes modulo 5, namely $n = 0, 1, 2, 3, 4$.

On the other hand, it is not the case that if $a \equiv b \mod n$ then

$$x^a \equiv x^b \mod n.$$

So in the case of the problem of showing that

$$5^n \equiv 1 \mod 4$$

the crucial point is

$$5 \equiv 1 \mod 4$$

i.e. the class of the base 5, not the class of the exponent.

You can show that $n^5 + 4n \equiv 0 \mod 5$ even faster if you use

Theorem (Fermat's little theorem). *If p is prime, and a is not a multiple of p, then $a^{p-1} \equiv 1 \mod p$.*

Proof. If a is not a multiple of p, it is a multiplicative unit in $\mathbb{Z}_p$, and so it suffices to show that

$$a^p \equiv a \mod p.$$

We shall show that this is the case *for all* a. This is clearly the case for $a = 0$. Suppose that a is a natural number, and $a^p \equiv a \mod p$. Then

$$\begin{aligned}(a+1)^p &\equiv \sum_{j=0}^{p} \binom{p}{j} a^j 1^{p-j} \mod p \\ &\equiv a^p + 1 \mod p \\ &\equiv a + 1 \mod p.\end{aligned}$$

$\square$

Recall that we used this to show

Exercise 1. Show that, if $a_1, \ldots, a_{30}$ are integers, not all divisible by 31, then

$$a_1^{30} + \cdots + a_{30}^{30}$$

is not divisible by 31.

Proof. Note that 31 is prime. By Fermat's Little Theorem, if a is not divisible by 31 then

$$a^{30} \equiv 1 \mod 31.$$

If not all the a_i are divisible by 31, then

$$\sum a_i^{30}$$

is congruent to a sum of thirty zeroes (the cases $a_i \equiv 0$) and ones, with at least one one. Therefore it is congruent to a nubmer between 1 and 30, and so not divisible by 31. $\square$

If a and b are relatively prime if and only if there are integers m and n so that

$$am + bn = 1.$$

Working modulo b, this says

Lemma 2. *a and b are relatively prime if and only if there is an integer m such that*

$$am \equiv 1 \mod b.$$

This is used in the proof of another big result of Chapter 7.

Theorem (Chinese remainder theorem). *If $\{n_1, \ldots, n_r\}$ is a set of r natural numbers that are pairwise relatively prime, and if $\{a_1, \ldots, a_r\}$ are any r integers, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ &\cdots \\ x &\equiv a_r \mod n_r \end{aligned}$$

has a unique solution modulo $N = \prod n_i$.

This is a good example of a proof which is an algorithm.

Proof. Let us show that if x and x' are solutions, then they must be congruent modulo N. Since

$$x \equiv x' \equiv a_i \mod n_i$$

we must have

$$n_i | (x - x').$$

Since the n_i are relatively prime, it follows that $N | (x - x')$, i.e. that

$$x \equiv x' \mod N.$$

We still need to show there's a solution. For each i, let

$$N_i = \frac{N}{n_i}.$$

Then since n_i is relatively prime to the other n_j, it follows that N_i and n_i are relatively prime. In other words, there is a unique congruence class Y_i such that $N_i Y_i \equiv 1 \mod n_i$. Choose a representative y_i (in applications, you can do this by the Euclidean Algorithm).

Set

$$x = \sum_j a_j N_j y_j.$$

Considered modulo n_i the terms with $j \neq i$ are congruent to 0 (because N_j is divisible by n_i). The i term gives

$$a_i N_i y_i \equiv a_i 1 \mod n.$$

$\square$

Application

Example 1. What is the smallest natural number n with the properties

$$
\begin{aligned}
n &\equiv 1 \mod 3 \\
n &\equiv 3 \mod 8 \\
n &\equiv 2 \mod 5?
\end{aligned}
$$

Solution

By the Chinese Remainder Theorem, there is a unique solution in Z_{120}. Thus there is a solution between 0 and 119, and it is smallest.

To find the solution, set

$$
\begin{aligned}
N_1 &= 40 \\
N_2 &= 15 \\
N_3 &= 24.
\end{aligned}
$$

Find y_i such that

$$
\begin{aligned}
N_1 y_1 &\equiv 1 \mod 3 \\
N_2 y_2 &\equiv 1 \mod 8 \\
N_3 y_3 &\equiv 1 \mod 5.
\end{aligned}
$$

For example

$$
\begin{aligned}
y_1 &= 1 \\
y_2 &= -1 \\
y_3 &= -1
\end{aligned}
$$

will do.

Then set

$$
\begin{aligned}
a_1N_1y_1 + a_2N_2y_2 + a_3N_3y_3 =& 1 \cdot 40 \cdot 1 + \\
& 3 \cdot 15 \cdot (-1) + \\
& 2 \cdot 24 \cdot (-1) \\
=& 40 - 45 - 48 \\
=& -53 \\
\equiv& 67 \quad \text{mod } 120.
\end{aligned}
$$

So the solution is 67.

For small examples, you could find the answer by enumeration. List the numbers congruent to 3 mod 8, and find the one that satisfies the other congruences. You need to check

$3, 11, 19, 27, 35, 43, 51, 59, 67, 75, 83, 91, 99, 107, 115$

Eliminate those divisible by 3 and 5 to shorten your list

$$11, 19, 43, 59, 67, 83, 91, 107$$

and check which are congruient to 2 mod 5

$$67, 107.$$

Only 67 is congruent to 1 mod 3.

Exercise 2. Find all solutions to the congruences

$$n \equiv 2 \mod 4$$
$$n \equiv 3 \mod 9.$$