Computer Science 70: Discrete Mathematics

The Chinese Remainder Theorem

The purpose of this note is to justify in detail our "formal" computation that

$$100^{50^{25^{10^5}}} \equiv 27 \pmod{47}.$$

Our main tool will be Euler's theorem, which we recall here:

Theorem (Euler's Theorem)**.** *Let a be relatively prime to N. Then*

$$a^{\varphi(N)} \equiv 1 \pmod{N},$$

where φ denotes the Euler totient function[1].

You proved this result, which is a straightforward generalization of Fermat's Theorem, in HW 4. We will need one other fact about modular arithmetic:

Theorem (Chinese Remainder Theorem)**.** *If m and n are relatively prime positive integers, the system of congruences*

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

has a unique solution (modulo mn).

Proof. We will prove uniqueness first. Suppose x_0 and x_1 are both solutions to the above system of congruences. Then

$$x_0 \equiv a \equiv x_1 \pmod{m}$$
$$x_0 \equiv b \equiv x_1 \pmod{n},$$

so in particular m divides $x_0 - x_1$ and n divides $x_0 - x_1$. Since m and n are relatively prime, this implies that mn divides $x_0 - x_1$ (check that you know why this is true), so $x_0 \equiv x_1 \pmod{mn}$.

To show existence, we will construct a solution x_0 explicitly. Since $\gcd(m, n) = 1$, m has an inverse x modulo n and n has an inverse y modulo m. Let

$$x_0 = any + bmx.$$

Then reducing this modulo m, we have

$$x_0 \equiv any \equiv a \pmod{m}$$

since $ny \equiv 1 \pmod{m}$, and similarly for the reduction of x_0 modulo n. Thus x_0 is the desired solution, and this proves the theorem. $\square$

[1] Recall that $\varphi(N)$ is the number of positive integers $n \leq N$ that are relatively prime to N

Remark. The Chinese Remainder Theorem easily generalizes to the case in which we have k linear congruences with the moduli of the congruences pairwise relatively prime. As an exercise, formulate precisely this generalization and prove your result.

We are now in a position to compute ("rigorously") the value of

$$100^{50^{25^{10^5}}} \pmod{47},$$

which we do in steps:

(1) We reduce the base modulo 47, so we're left with the computation of

$$6^{50^{25^{10^5}}} \pmod{47}.$$

(2) **Subproblem.** We can reduce the exponent modulo 46 by Fermat's theorem (since $p = 47$ is prime), so we want to compute

$$50^{25^{10^5}} \equiv 4^{25^{10^5}} \pmod{46}.$$

While we'd like to compute this by reducing the exponent 25^{10^5} mod $\varphi(46) = 22$, we can't exactly do this since Euler's theorem doesn't apply—46 and 4 are not relatively prime. Instead, we solve the system of linear congruences given by

$$x \equiv 4^{25^{10^5}} \pmod{23}$$
$$x \equiv 4^{25^{10^5}} \pmod{2}.$$

(3) **Subproblem.** To compute

$$4^{25^{10^5}} \pmod{23}$$

we can apply Fermat's theorem to reduce 25^{10^5} modulo 22, and to compute this we can apply Euler's theorem to reduce 10^5 modulo $\varphi(22) = (11-1)(2-1) = 10$. But $10^5 \equiv 0 \pmod{10}$, so $25^{10^5} \equiv 1 \pmod{22}$, so

$$4^{25^{10^5}} \equiv 4 \pmod{23}.$$

(4) Since

$$4 \equiv 4^{25^{10^5}} \pmod{2}$$

trivially, we know that 4 is a solution to the system of linear congruences. Since

$$4^{25^{10^5}}$$

is also a solution, we can conclude (by the uniqueness statement of the Chinese Remainder Theorem) that

$$4^{25^{10^5}} \equiv 4 \pmod{46}.$$

(5) Thus, back at the highest level, we're left with the computation of

$$6^4 \pmod{47},$$

which one easily finds is 27.

Since we didn't discuss it in class, you weren't expected to know the Chinese Remainder Theorem for the midterm: continually applying Euler's theorem (without regard to the technicality in step 2 above) would have given you the same answer, and this is what we had wanted you to do.