M328K – Rusin – HW2 ANSWERS – Due Thursday, Feb 2 2017

1. Compute $7^{160} \pmod{11}$. Your answer should be one of the numbers

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\quad or \quad 10.$$

ANSWER: The first few powers of 7 are congruent (modulo 11) to: $7^0 \equiv 1, 7^1 \equiv 7, 7^2 = 49 \equiv 5, 7^3 \equiv 7 \cdot 5 = 35 \equiv 2, 7^4 \equiv 7 \cdot 2 = 14 \equiv 3, 7^5 \equiv 7 \cdot 3 = 21 \equiv -1$. Then $7^{10} = (7^5)^2 \equiv (-1)^2 = 1$, so $7^{160} = (7^{10})^{16} \equiv 1$, too.

We would later learn Fermat's Little Theorem, that for any a and any prime p we have $a^p \equiv a \pmod{p}$. Multiplying both sides by the inverse of a (when it has one mod p) then shows $a^{p-1} \equiv 1$. We just verified this fact the slow way when $p = 11, a = 7$.

2. Show that if $a \equiv b \pmod{c}$ and $d \equiv f \pmod{c}$ then $ad \equiv bf \pmod{c}$

ANSWER: We are given that $a = b + cm$ for some m and that $d = f + cn$ for some n. Thus $ad = (b + cm)(f + cn) = (bf) + c(mf + nb + cnm) \equiv bf \pmod{c}$.

This is the beauty of modular thinking: if you don't care about all those multiples of c, why drag them around? We just get to focus on the a, b, d, f.

3. True or false? If a, b, c, d are positive integers and $a \equiv b \pmod{c}$ and $a \equiv b \pmod{d}$ then $a \equiv b \pmod{cd}$. (Prove or give a counterexample.)

ANSWER: False. Try $a = 30, b = 0, c = 6, d = 10$.

But the result IS true if c and d are coprime. Indeed, we are given that $a - b$ is a common multiple of both c and d. It's then not hard to see that $a - b$ is a multiple of the lcm of c and d (their *least common multiple*). In particular, if c and d have no common factor at all, then their lcm is just cd and the claimed result would be true. (In the example I gave, $a \not\equiv b \pmod{cd}$ but it IS true that $a \equiv b$ modulo the lcm of c and d, which is 30.)

4. List all the divisors that the numbers 75 and 45 have in common (and therefore deduce what is the gcd of 45 and 75).

ANSWER: Since $75 = 3 \cdot 5^2$, all the divisors of 75 are the numbers $3^i 5^j$ with $0 \le i \le 1$ and $0 \le j \le 2$, that is (if I can make up notation on the fly) it's the set $\{1 \text{ or } 3\} \times \{1 \text{ or } 5 \text{ or } 25\} = \{1, 3, 5, 15, 25, 75\}$. Likewise the divisors of $45 = 3^2 \cdot 5$ are $\{1 \text{ or } 3 \text{ or } 9\} \times \{1 \text{ or } 5\} = \{1, 3, 9, 5, 15, 45\}$ These two sets have only $\{1, 3, 5, 15\}$ in common so the gcd is 15.

In general, the gcd of $2^{n_2} \cdot 3^{n_3} \cdot 5^{n_5} \cdot \ldots$ and $2^{m_2} \cdot 3^{m_3} \cdot 5^{m_5} \cdot \ldots$ is $2^{k_2} \cdot 3^{k_3} \cdot 5^{k_5} \cdot \ldots$, where for each prime p, k_p is the lesser of m_p and n_p.

5. Show that if a is any integer, then $a^3 - a$ is a multiple of 3.

ANSWER: Here again I was anticipating Fermat's theorem but you can prove this directly: $a^3 - a = (a - 1)a(a + 1)$ is a product of three consecutive integers, one of which must then be a multiple of 3, making $a^3 \equiv a \pmod{3}$ too. Or you can use a proof by induction: $1^3 - 1$ is a multiple of 3 and $(a + 1)^3 - (a + 1) = (a^3 - a) + 3(a^2 + a)$, so the left side is a multiple of 3 iff $a^3 - a$ is. That's the inductive observation that completes the proof by induction.