In-Class Problems Week 8, Mon.

Problem 1. **(a)** Let $m = 2^9 5^{24} 11^7 17^{12}$ and $n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2$. What is the $\gcd(m,n)$? What is the *least common multiple*, $\text{lcm}(m,n)$, of m and n? Verify that

$$\gcd(m,n) \cdot \text{lcm}(m,n) = mn. \tag{1}$$

(b) Describe in general how to find the $\gcd(m,n)$ and $\text{lcm}(m,n)$ from the prime factorizations of m and n. Conclude that equation (1) holds for all positive integers m, n.

Problem 2. The following properties of equivalence mod n follow directly from its definition and simple properties of divisibility. See if you can prove them without looking up the proofs in the notes.

(a) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

(b) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(c) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

(d) $\text{rem}(a,n) \equiv a \pmod{n}$.

Problem 3. **(a)** Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9? *Hint:* $10 \equiv 1 \pmod{9}$.

(b) Take a big number, such as 37273761261. Sum the digits, where every other one is negated:

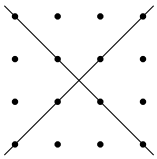
$$3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 = -11$$

Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11. *Hint:* $10 \equiv -1 \pmod{11}$.

Problem 4. Two nonparallel lines in the real plane intersect at a point. Algebraically, this means that the equations

$$y = m_1 x + b_1$$
$$y = m_2 x + b_2$$

have a unique solution (x, y), provided $m_1 \neq m_2$. This statement would be false if we restricted x and y to the integers, since the two lines could cross at a noninteger point:



However, an analogous statement holds if we work over the integers *modulo a prime*, p. Find a solution to the congruences

$$y \equiv m_1 x + b_1 \pmod{p}$$
$$y \equiv m_2 x + b_2 \pmod{p}$$

when $m_1 \not\equiv m_2 \pmod{p}$. Express your solution in the form $x \equiv ? \pmod{p}$ and $y \equiv ?? \pmod{p}$ where the ?'s denote expressions involving m_1, m_2, b_1, and b_2. You may find it helpful to solve the original equations over the reals first.

Appendix

Definition. $a \equiv b \pmod{n}$ iff $n \mid a - b$.

Lemma 4.1. *[Facts About Congruences] The following hold for $n \geq 1$:*

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ *implies* $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ *implies* $a \equiv c \pmod{n}$
4. $a \equiv \text{rem}(a, n) \pmod{n}$
5. $a \equiv b \pmod{n}$ *implies* $a + c \equiv b + c \pmod{n}$
6. $a \equiv b \pmod{n}$ *implies* $ac \equiv bc \pmod{n}$
7. $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *imply* $a + c \equiv b + d \pmod{n}$
8. $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *imply* $ac \equiv bd \pmod{n}$

Lemma 4.2 (Inverses mod n)**.** *If k and $n > 1$ are relatively prime, then there is a positive integer $k^{-1} < n$ called the* modulo n inverse *of k, such that*

$$k \cdot k^{-1} \equiv 1 \pmod{n}.$$

Proof. That integers k and n are relatively prime means that $\gcd(k, n) = 1$. But $\gcd(k, n) = 1$ implies that $1 = ak + bn$ for some integers a, b, and so $1 \equiv ak \pmod{n}$. So the positive integer less than n that is equivalent to $a \pmod{n}$ is k^{-1}, namely, $k^{-1} = \text{rem}(a, n)$. □