MAT 311 Introduction to Number Theory

# Problem Set 4

Some Solutions

**Problem 1.** Solve the following systems of congruences.

(a) $x \equiv 3 \mod 5$
$x \equiv 2 \mod 8$
$x \equiv 0 \mod 7$

(b) $13x \equiv 2 \mod 15$
$16x \equiv 3 \mod 25$

(c) $x \equiv 0 \mod 18$
$3x \equiv 12 \mod 20$
$2x \equiv -2 \mod 30$

**Solution.** (a) All moduli are pairwise relatively prime, so by the Chinese remainder theorem the system has a unique solution $\mod 5 \cdot 8 \cdot 7 = 280$. From the last congruence, $x = 7k$, then from the first two we get $2k \equiv 3 \mod 5$ and $-k \equiv 2 \mod 8$. The first of these is equivalent to $k \equiv 4 \mod 5$. To solve $k \equiv 4 \mod 5$ and $k \equiv -2 \mod 8$, we can guess $k = 14$ or follow the strategy from the Chinese remainder theorem: find $a, b$ such that $8a \equiv 1 \mod 5$ and $5b \equiv 1 \mod 8$. We can take $a = 2$ and $b = 5$. Then $k = 4 \cdot 8 \cdot a + (-2) \cdot 5 \cdot b = 64 - 50 = 14$ is a solution. Then $x = 7 \cdot 14 = 98$ is a solution, and all solutions are given by $98 + 280m$, $m$ integer. (Many other solutions are possible.)

(b) $13x \equiv 2 \mod 15$ implies $13x \equiv 3x \equiv 2 \mod 5$; $16x \equiv 3 \mod 25$ implies $16x \equiv x \equiv 3 \mod 5$. But if $x \equiv 3 \mod 5$, then $3x \equiv 9 \equiv 4 \mod 5$, which contradicts $3x \equiv 2 \mod 5$, so there are no solutions.

Similarly, in (c) $x \equiv 0 \mod 18$ implies $3|x$ which contradicts $2x \equiv -2 \mod 30$. No solutions either.

**Problem 2.** Prove that $7|(3^{2n+1} + 2^{n+2})$ for all $n$.

**Solution.** $3^{2n+1} + 2^{n+2} = 3 \cdot (3^2)^n + 4 \cdot 2^n \equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \mod 7$.

**Problem 3.** For what $n$ is $\phi(n)$ odd?

**Solution.** Only for $n = 2$. Indeed, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then $\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_1^{\alpha_2 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$. If at least one of $p_i$ is odd, then both $p_i^{\alpha_i}$ and $p_i^{\alpha_i - 1}$ are odd, so $p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ is even and $\phi(n)$ is even. If $n = 2^m$, $\phi(n)$ is also even unless $m = 1$.

**Problem 4.** Prove that

$$(p-1)! \equiv p - 1 \mod (1 + 2 + 3 + \dots + (p-1)) \text{ if } p \text{ is prime.}$$

**Solution.** Assume $p > 2$, as the case $p = 2$ is trivial. We have $1+2+3+\dots+(p-1) = p\frac{p-1}{2}$. (The sum of all integers from 1 to $n$ is $\frac{n(n+1)}{2}$. You can prove this by induction or by adding numbers in pairs, $1+n$, $2+(n-1)$, etc.) Note that since $p > 2$ is prime, $\frac{p-1}{2}$ is an integer. Besides, $p$ and $\frac{p-1}{2}$ are relatively prime. Then the congruence $p-1)! \equiv p - 1 \mod p\frac{p-1}{2}$ is equivalent to the system of two congruences, $(p-1)! \equiv p - 1 \mod p$ and $(p-1)! \equiv p - 1 \mod \frac{p-1}{2}$. The first one follows from Wilson's theorem ($(p-1)! \equiv -1 \mod p$); the second, $(p-1)! \equiv p - 1 \equiv 0 \mod \frac{p-1}{2}$, holds because $p - 1$ divides $(p-1)!$

**Problem 5.** (a) Find the last digit of $2^{1000}$ and the last digit of $3^{1000}$.

**Solution.** For this, it suffices to look at last digits of $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64...$ and notice that the last digit will repeat cyclically in the pattern $2, 4, 8, 6, 2, 4, 8, 6.....$ Because $4|1000$, the last digit of $2^{1000}$ will be 6. Similarly, for powers of 3 we have $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81$, $3^5 = ..3$, so the cyclical pattern is $3, 9, 7, 1, 3, 9, 7, 1, 3..$, and the last digit of $3^{1000}$ is 1.

(b) Find the last two digits of $3^{1000}$.

**Solution.** The last two digits are given by $3^{1000} \mod 100$. Since 3 and 100 are relatively prime, Euler's theorem applies, so $3^{\phi(100)} \equiv 1 \mod 100$. Compute $\phi(100) = \phi(2^2)\phi(5^2) = (4-2)(25-5) = 40$. So $3^{40} \equiv 1 \mod 100$, and then $3^{1000} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1 \mod 100$, so the last two digits are 01.

(c) Find the last two digits of $2^{1000}$.

**Solution.** Since 2 and 100 are not relatively prime, Euler's theorem with $\phi(100)$ won't apply. However, we can argue that $2^{\phi(25)} = 2^{20} \equiv 1 \mod 25$, so $2^{1000} \equiv (2^{20})^5 0 \equiv 1 \mod 25$. This gives 4 possibilities for the last 2 digits: 01, 26, 51, 76. Since we also know that $4|2^{1000}$, the last two digits must be 76.