Math 40520 Theory of Number
Homework 4

Due Friday 9/28, in class

Main topics: Euler's theorem, Euler's φ, Chinese Remainder Theorem, primitive roots for $\mathbb{Z}_p^\times$ and $\mathbb{Z}_{p^k}^\times$, integers in bases other than 10, multiplicative orders.

Do 5 of the following problems.

1. Show that if $m \mid n$ then $\varphi(m) \mid \varphi(n)$.

2. Let n be a number such that $n+1$ is divisible by 24. If $d \mid n$ show that 24 divides $d^2 - 1$.

3. Compute
$$12^{34^{56^{78}}} \mod 90$$
[Hint: It is much easier to use Euler's theorem in conjunction with the Chinese Remainder Theorem.] (The author of this problem was very proud of having used each digit exactly once. This idiosyncrasy actually makes the problem easier.)

4. Show that the polynomial $P(X) = (X^2-2)(X^2-3)(X^2-6)$ has no integral roots but has roots mod p for every prime p.

5. Let p be a prime number and a an integer coprime to p. Show that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ with 1 if and only if there exists b such that $a \equiv b^2 \pmod{p}$.

6. Let $p \equiv 3 \pmod 4$ be a prime number. Suppose you know that $y \equiv x^2 \pmod 4$ for some $x \in \mathbb{Z}_p^\times$. Show that $x \equiv \pm y^{(p+1)/4} \pmod{p}$.

7. Suppose $p > 2$ is a prime, $n \geq 2$ and a is an integer such that a is a primitive root modulo p^2. Show that a is then also a primitive root modulo p^n for all n. [Hint: Show that $a^{p-1} \equiv 1 + p \cdot b \pmod{p^2}$ where $b \not\equiv 0 \pmod p$.]

8. Let a be a positive integer. Find the smallest positive integer k such that $2^{2018} \mid a^k - 1$. [Hint: Review how we computed the multiplicative order of 3 mod 2^n then write a in binary.]

9. (Bonus exercise. This is not a hard exercise, even if it looks very long.) In this exercise you will multiply two positive integers using only doubling, halving and additions. Suppose m and n are two positive integers. Put m and n on the same row in a table with two columns. You will iterate the following operation. Taking the last row of the column, multiply by 2 the left entry and divide by 2 the right entry and put the new values on the next row, forgetting about decimals. When the right row becomes 0, stop the iteration. Eliminate from the column every row in which the right entry is even, then add all the remaining left entries. This sum will then be the product $m \cdot n$. For example

$x \times 2$	$\lfloor x/2 \rfloor$
23	25
~~46~~	~~12~~
~~92~~	~~6~~
184	3
368	1
~~736~~	~~0~~

yield $23 \cdot 25 = 575 = 368 + 184 + 23$.

(a) Write $m = \overline{m_1 m_2 \cdots m_k}_{(2)}$ and $n = \overline{n_1 n_2 \ldots n_k}_{(2)}$ in base 2. Show that the table, all entries written in base 2, is

$x \times 2$	$\lfloor x/2 \rfloor$
$\overline{m_1 m_2 \cdots m_k}$	$\overline{n_1 n_2 \ldots n_k}$
$\overline{m_1 m_2 \cdots m_k 0}$	$\overline{n_1 n_2 \ldots n_{k-1}}$
$\overline{m_1 m_2 \cdots m_k 00}$	$\overline{n_1 n_2 \ldots n_{k-2}}$
$\vdots$	$\vdots$
$\overline{m_1 m_2 \cdots m_k \underbrace{00\ldots0}_{k-1}}$	$\overline{n_1}$
$\overline{m_1 m_2 \cdots m_k \underbrace{00\ldots0}_{k}}$	0

(b) Show that the algorithm is correct. [Hint: Write out multiplication in base 2.]