Due July 8, 11:59pm on Gradescope.

The following are warm-up exercises and are *not* to be turned in. You may treat these as extra practice problems.

4.3.18, 4.3.22, 4.3.37, 4.3.41, 4.4.7, 4.4.8, 4.4.17, 4.4.40, 4.4.41, 4.4.48.

Turn in the following exercises. Remember to carefully justify every statement that you write, and to follow the style of proper mathematical writing. You may cite any result proved in the textbook or lecture, unless otherwise mentioned. Each problem is worth 10 points with parts weighted equally, unless otherwise mentioned.

1. **(5 points)** 4.3.54.

2. Some numerical examples:

   (a) **(3 points)** 4.4.20. Express your answer as a single congruence condition: that is, your answer should be of the form "the solutions are exactly those integers of the form $x \equiv a \bmod m$," where $0 \leq a < m$ are integers for you to determine.

   (b) **(3 points)** Find all prime numbers p such that $7p^2 + 20$ is also prime.

   (c) **(4 points)** Let a be the unique integer in $[0, 1000]$ such that a is an inverse of 4^{598} mod 1001. Find a. [Hint: $1001 = 7 \cdot 11 \cdot 13$.]

3. We say that an integer is *squarefree* if it is not divisible by any perfect squares other than 1. Show that for any positive integer k, there exist k consecutive positive integers, none of which are squarefree.

4. **(25 points)** The *Euler totient function* φ is defined as follows: for a positive integer n, $\varphi(n)$ is the number of positive integers $1 \leq m \leq n$ such that $(m, n) = 1$. For example, brute-force checks show that $\varphi(3) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, and $\varphi(10) = 4$.

   (a) **(5 points)** 4.3.23.

   (b) **(10 points)** Using the Chinese remainder theorem, show that if a and b are coprime positive integers, then $\varphi(a)\varphi(b) = \varphi(ab)$. [Hint: Let S_n be the set $\{m \in \mathbf{Z} : 1 \leq m \leq n, (m, n) = 1\}$, so $\varphi(n) = |S|$. Construct a bijection from $S_a \times S_b$ to S_{ab}.] Therefore by induction, if $a_1, a_2, \ldots, a_r$ are pairwise coprime integers, and a is their product, then $\varphi(a) = \prod_{i=1}^{r} \varphi(a_i)$. [Since we haven't formally talked about induction yet, you do not need to prove this statement.]

(c) **(5 points)** Using parts (a) and (b), deduce that if a positive integer n has the unique prime factorization

$$n = \prod_{i=1}^{r} p_i^{a_i}$$

for distinct primes $p_1, p_2, \ldots, p_r$ and positive integers $a_1, a_2, \ldots, a_r$, then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(d) **(5 points)** Compute $\varphi(70000)$.

Remark: The totient function gives the following generalization (Euler's Theorem) of Fermat's Little Theorem: suppose m is any integer greater than 1 (possibly composite), and a an integer such that $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \bmod m$. This can be proved via the same method we used for Fermat's little theorem.

5. **(35 points)** Let p be a prime number and a a nonzero element in $\mathbf{Z}/p\mathbf{Z}$. In this exercise, all arithmetic operations take place in $\mathbf{Z}/p\mathbf{Z}$ (e.g. so if $p = 3$, then $2^2 = 1$). If n is the smallest positive integer such that $a^n = 1$, we call n the *order of a mod p*, and we denote it by $\mathrm{ord}_p(a)$.

   (a) **(5 points)** Compute $\mathrm{ord}_7(2)$ and $\mathrm{ord}_{11}(3)$.

   (b) **(10 points)** Show that for any nonzero $a \in \mathbf{Z}/p\mathbf{Z}$ and k is a positive integer such that $a^k = 1$, then $\mathrm{ord}_p(a) | k$. Deduce that $\mathrm{ord}_p(a) | (p-1)$ for all nonzero $a \in \mathbf{Z}/p\mathbf{Z}$.

   (c) **(10 points)** Show that such an a is a primitive root of $\mathbf{Z}/p\mathbf{Z}$ if and only if $\mathrm{ord}_p(a) = p - 1$. [Hint: think about the function $f : [p-1] \to \mathbf{Z}/p\mathbf{Z} - \{0\}$ given by $n \mapsto a^n$.]

   (d) **(10 points)** Using the fact that $\mathbf{Z}/p\mathbf{Z}$ has a primitive root, show that if d is a positive integer dividing $p - 1$, there are exactly d elements in $\mathbf{Z}/p\mathbf{Z}$ satisfying the equation $x^d = 1$. In other words, any integer y satisfying the congruence $y^d \equiv 1 \bmod p$ is equivalent to one of d canonical residue classes (i.e. one of d integers in $[0, p-1]$).

   Remark: In fact, part (d) is slightly circular, in the following sense: the *proof* that $\mathbf{Z}/p\mathbf{Z}$ has a primitive root uses the fact that there are exactly d elements in $\mathbf{Z}/p\mathbf{Z}$ satisfying the equation $x^d = 1$ as an intermediate step (and this step is of course deduced without a circular assumption that $\mathbf{Z}/p\mathbf{Z}$ has a primitive root). Unfortunately, that proof is too long to include as an exercise (even though we have most of the tools we need).

6. **(15 points)** If m is a positive integer, and if a is an integer coprime to m, then a is a *quadratic residue* mod m if there exists a solution to the congruence $x^2 \equiv a \bmod m$ (i.e. a

is a perfect square mod m). We usually take m to be a prime. For instance, the quadratic residues mod 7 are congruent to 1, 2, and 4, because the (nonzero) perfect squares mod 7 are:

$$1^2 \equiv 1 \bmod 7, 2^2 \equiv 4 \bmod 7, 3^2 \equiv 2 \bmod 7, 4^2 \equiv 2 \bmod 7, 5^2 \equiv 4 \bmod 7, 6^2 \equiv 1 \bmod 7.$$

If p is an odd prime and $(a, p) = 1$, then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue mod p, and -1 otherwise. So for instance, $\left(\frac{a}{7}\right)$ equals 1 if $a = 1, 2, 4, 8, -5, -3$, etc., and it equals -1 if $a = 3, 5, 6, 17, -9, -1$, etc.

(a) **(10 points)** 4.4.62. [Alternative hint for the case when a is not a quadratic residue: Problem 5(d).]

(b) **(5 points)** 4.4.64.

Remark: The following is the beautiful and surprisingly deep result known as *quadratic reciprocity*: for any odd primes p and q, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Thus whether p is a square mod q is directly connected to whether q is a square mod p!

7. **(Bonus problem, 10 points)** Show that there are no solutions in integers to the *elliptic curve* given by $y^2 = x^3 - 9$.

8. **(Bonus problem, 20 points)** Let a_1, a_2, a_3, a_4, n be integers such that $n > 1$ and $a_1a_2 - a_3a_4 \equiv 1 \bmod n$. Show that there are integers b_1, b_2, b_3, b_4 such that $a_i \equiv b_i \bmod n$ for each $1 \leq i \leq 4$, and $b_1b_2 - b_3b_4 = 1$.