1. In class we distinguished between two properties for a number n: n is *irreducible* if its only positive factors are 1 and n, and n is *prime* if whenever n divides a product ab it must divide either a or b. In class we proved that every irreducible number is prime (this was "Euclid's Lemma"). I said that the two properties were equivalent, but we didn't prove the other direction. So:

Prove that every prime number is irreducible.

2. There is a rule for testing divisibility by 13 much like the rule for testing divisibility by 7. If $n = a_k a_{k-1} \cdots a_0$ is the decimal expansion of n (e.g., $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$) then $13|n$ if and only if 13 divides $\frac{n-a_0}{10} + 4a_0$.

(a) Use the rule to check if $n = 32032$ is divisible by 13.

(b) Prove that the rule is correct.

3. Another divisibility test for 7 involves taking the alternating sum of digits in groups of three, with the sign positive for the lowest group of three. As an example

$$n = 1987446881 \equiv -1 + 987 - 446 + 881 = 1421 \equiv -1 + 421 = 420 \pmod 7.$$

Since 420 is divisible by 7, we conclude that 1987446881 is divisible by 7.

Surprisingly, the same reductions also work for 11 and 13: $1987446881 \equiv 420 \pmod{11}$ and $1987446881 \equiv 420 \pmod{13}$.

Prove that for any positive integer n, $n \equiv$ (alternating sum of groups of three digits) $\pmod p$ if $p = 7$, 11, or 13.

4. Modular arithmetic can transform many questions that seem opaque into questions that are quite easy to answer. Consider the statement below:

If $p \geq 5$ is a prime number, then $p^2 + 2$ is always a composite number.

Without looking ahead, think about how you would try and approach demonstrating this. Does it seem very easy?

Now:

(a) List the squares mod 3.

(b) Prove that if k is not a multiple of 3, then 3 divides $k^2 + 2$.

(c) Prove that if p is a prime number and $p \geq 5$ then $p^2 + 2$ is a composite number.

5. Some more modular arithmetic.

(a) Compute the remainders of 7, 7^2, 7^3, 7^4, 7^5, and 7^6 when divided by 19.

(b) Compute the remainder of 7^{2008} when divided by 19.

(c) Compute the remainders of 8, 8^2, 8^3, 8^4, 8^5, and 8^6 when divided by 19.

(d) Compute the remainder of 8^{2008} when divided by 19.

(e) Compute the remainder of 56^{2008} when divided by 19.

HINTS:

1. Finding the remainder when dividing by 19 is another way of talking about computing mod 19.
2. Calculations mod 19 behave well with respect to arithmetic operations (multiplying, taking powers, etc).
3. So you should definitely *not* be raising any number to the power 2008 and then computing the remainder.
4. $56 = 7 \cdot 8$.