Homework 3

Math 467 Due: 9 September, 2016

1.

a) Show that if $a, b \in \mathbb{N}$ have remainders in the set $\{1, 4\}$ after division by 5, then so does their product.

b) Show that there are infinitely many primes which have remainders 2 or 3 when divided by 5.

Hint: Imitate the proof of Euclid's Theorem by forming a product involving primes (each with remainder 1 or 4) and possibly something else so that when we add, say, 2, we obtain a number N with remainder 2 after division by 5. Then apply part a).

2. Set F_n denote the nth Fermat number $F_n = 2^{2^n} + 1$.

a) Show that if $m < n$, then F_m divides $F_n - 2$.

b) Deduce once more that there exist infinitely many primes.

Hint: We have seen in class that $b^k + 1 \mid b^{2k} - 1$ and that, when $k \mid l$, $b^k - 1 \mid b^l - 1$.

3. Implement our Algorithm 5, the Sieve of Eratosthenes, and find all the primes between 1600 and 3600.

How many pairs of primes differ by 2?

4. Prove by a careful induction that if $r \in \mathbb{N}$, then

$$b^{2^r} - 1 = (b-1)(b+1)(b^2+1)(b^{2^2}+1)\cdots(b^{2^{r-1}}+1).$$

You may use either the Well-Ordering Principle or standard Mathematical Induction.

5. Let $a \equiv r \mod m$ and $b \equiv s \mod m$. Prove the following:

(a) $a + b \equiv r + s \mod m$.

(b) $ab \equiv rs \mod m$.

(c) Generalize the proof of Euclid's Lemma to show that if $\gcd(a, m) = 1$ and $ac \equiv 0 \mod m$, then $c \equiv 0 \mod m$.

(d) Conclude that if $\gcd(a, m) = 1$ and $ab \equiv ac \mod m$, then $b \equiv c \mod m$.