Math 3240 - Introduction to Number Theory — Due by email
Problem Set 3 — 3/14/20 at Noon

> *I think that I have always had a basic liking for the natural numbers. To me they are the one real thing. We can conceive of a chemistry which is different from ours, or a biology, but we cannot conceive of a different mathematics of numbers. What is proved about numbers will be a fact in any universe.* Julia Robinson

Required Reading: Handouts on Infinitude of Primes, Patterns in Primes, and Fermat's Little Theorem.

1. (Induction practice)

   Say a function $f\colon \mathbf{R} \to \mathbf{R}$ has *period* n, where n is a positive integer, if $f(t+n) = f(t)$ for all $t \in \mathbf{R}$. For example, $\sin(\pi t)$ and $\cos(\pi t)$ have period 2 since, for all $t \in \mathbf{R}$, $\sin(\pi(t+2)) = \sin(\pi t + 2\pi) = \sin(\pi t)$ and $\cos(\pi(t+2)) = \cos(\pi t + 2\pi) = \cos(\pi t)$.

   a) (**10 pts**) If $f\colon \mathbf{R} \to \mathbf{R}$ has period n, then prove (i) $f(t-n) = f(t)$ for all $t \in \mathbf{R}$ and (ii) for each $t \in \mathbf{R}$, $f(t+nk) = f(t)$ for all $k \in \mathbf{Z}$ (positive, negative, and 0) using induction on k.

   b) (**10 pts**) Use part a to help you prove that if $f\colon \mathbf{R} \to \mathbf{R}$ has periods n_1 and n_2 then it has period (n_1, n_2). That is, if $f(t+n_1) = f(t)$ and $f(t+n_2) = f(t)$ for all $t \in \mathbf{R}$, then $f(t+(n_1,n_2)) = f(t)$ for all $t \in \mathbf{R}$. (For example, if $f(t+30) = f(t)$ and $f(t+78) = f(t)$ for all $t \in \mathbf{R}$ then $f(t+6) = f(t)$ for all $t \in \mathbf{R}$.)

2. (More simultaneous congruences)

   a) (**10 pts**) Use the method from class to write the two congruence conditions $x \equiv a \bmod 12$ and $x \equiv b \bmod 91$ for fixed $a, b \in \mathbf{Z}$ as a single congruence condition on x modulo $12 \cdot 91$. (The final answer will depend on a and b.) Then **check your answer really works**. You can use Wolfram Alpha or any other computer algebra package to find inverses in modular arithmetic.

   b) (**10 pts**) In $\mathbf{Q}[T]$, write the two congruence conditions $f(T) \equiv a(T) \bmod T^2 + T$ and $f(T) \equiv b(T) \bmod T^3 - 2$ for fixed $a(T), b(T) \in \mathbf{Q}[T]$ as a single congruence condition on $f(T)$ modulo $(T^2+T)(T^3-2)$. (The final answer will depend on $a(T)$ and $b(T)$.) Then **check your answer really works**. Use Euclid's algorithm to find inverses in modular arithmetic.

3. (Fermat witnesses)

   a) (**10 pts**) Use Wolfram Alpha or any other computer algebra system to find the smallest Fermat witness for 2701. Separately, determine the binary representation of 2700 and use that to describe how many multiplications are sufficient to compute a^{2700} for an integer a (it is far less than 2700).

   b) (**10 pts**) Let $m = 56052361$. Using Wolfram Alpha or any other computer algebra system, determine if 2, 3, 5, 6, 7, 10, or 11 are Fermat witnesses for m. What do you find? Does this alone tell you with certainty whether m is prime or composite, and why?

4. Determine which of the following prime patterns should occur infinitely often according to the conjectures discussed in class.

   a) (**2 pts**) $p, p+3, p+5$

   b) (**3 pts**) $p, p+2, p+6, p+8$

   c) (**3 pts**) $p, p+2, p+10, p+12$

   d) (**3 pts**) $3n+2, 4n+3, 5n+1$

   e) (**3 pts**) n^3+n+5

   f) (**3 pts**) n^2-11

   g) (**3 pts**) n^3+n+5, n^2-11

5. (Exploration)

Look at the files "Squares Modulo Primes" and "Congruence Conditions on Primes" *together*, which both tabulate information about the primes less than 200. From that data, it appears that

$$-1 \equiv \square \bmod p \iff p = 2 \text{ or } p \equiv 1 \bmod 4,$$

where $\square \bmod p$ means "square modulo p". The right side describes all $p < 200$ for which $-1 \equiv \square \bmod p$ *and* does not include any $p < 200$ for which $-1 \not\equiv \square \bmod p$.

Conjecture a similar description in terms of congruences on p for each of the six conditions

a) (**3 pts**) $2 \equiv \square \bmod p$:

b) (**3 pts**) $-2 \equiv \square \bmod p$,

c) (**4 pts**) $3 \equiv \square \bmod p$,

d) (**3 pts**) $-3 \equiv \square \bmod p$,

e) (**3 pts**) $5 \equiv \square \bmod p$,

f) (**4 pts**) $-5 \equiv \square \bmod p$.

The last case will be harder than the rest! (Your conditions should describe the intended primes and *not* others, *e.g.*, $p \equiv 1, 5 \bmod 6$ is useless since it describes all primes but 2 and 3.)