1. a) Find the first four $n > 1$ such that $6n + 1$, $12n + 1$, and $18n + 1$ are all prime.

   b) If $6n+1$, $12n+1$, and $18n+1$ are prime for an $n \geq 1$ then prove $N := (6n+1)(12n+1)(18n+1)$ is a Carmichael number: $a^{N-1} \equiv 1 \bmod N$ for all a that are relatively prime to N.

2. When m is composite and not a Carmichael number (there is a solution to $a^{m-1} \not\equiv 1 \bmod m$ with $(a, m) = 1$), it was stated in the lecture that the proportion of Fermat witnesses for m in $\{1, 2, \ldots, m-1\}$ is greater than 50%. Can 50%, as a common lower bound, be improved?

   a) Show Hypothesis H implies p and $2p - 1$ are both prime together infinitely often.

   b) If p and $2p-1$ are both odd primes, let $m = p(2p-1)$. Prove exactly half the units a mod m satisfy $a^{m-1} \equiv 1 \bmod m$ and deduce from this that

$$\frac{|\{1 \leq a \leq m-1 : a^{m-1} \not\equiv 1 \bmod m\}|}{m-1} = \frac{m-1-\varphi(m)/2}{m-1} = \frac{p+2}{2p+1},$$

   which tends to $1/2$ (from above) if we can let $p \to \infty$. (Hint: $m - 1$ has a nice factorization.)

3. For each integer a that is not -1 or a perfect square, show Hypothesis H with two well-chosen linear polynomials (depending on a) implies a generates U_p for infinitely many primes p.

4. A *primitive Pythagorean triple* is a triple of positive integers (a, b, c) such that $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$. Either a or b must be even. Such triples with b even can be described as $(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$ where $m > n > 0$, $(m, n) = 1$, and $m \not\equiv n \bmod 2$.

   a) If two of the three terms in a primitive Pythagorean triple are prime, show $m = n + 1$ and the triple is $(2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$.

   b) Prove the set $\{2T + 1, 2T^2 + 2T + 1\}$ satisfies the conditions of Hypothesis H.

   c) When n is 1 and 2, the triple in part a is $(3, 4, 5)$ and $(5, 12, 13)$. Find the next four $n > 2$ for which the triple in part a has two of its terms being prime numbers.

5. Bunyakovsky's condition makes sense for integer-valued polynomials, but is the equivalence in 3d on Set 1 true for such polynomials? Care is needed since for integer-valued polynomials $f(T)$ we have $a \equiv b \bmod c \not\Rightarrow f(a) \equiv f(b) \bmod c$ in general. (Try $f(T) = (T^2 + T)/2$ with $a = 0$, $b = 2$, and $c = 2$.)

   Let $k \in \mathbf{N}$ and p be a prime number.

   a) If $p^r > k$, prove for all $a, b \in \mathbf{Z}$ that $a \equiv b \bmod p^r \Longrightarrow \binom{a}{k} \equiv \binom{b}{k} \bmod p$. Note the modulus at the end is p, not p^r. (Hint: Use the polynomial identity $\binom{X+Y}{k} = \displaystyle\sum_{i=0}^{k} \binom{X}{i}\binom{Y}{k-i}$.)

   b) If $p^r \leq k$ find integers a and b such that $a \equiv b \bmod p^r$ and $\binom{a}{k} \not\equiv \binom{b}{k} \bmod p$.

   c) Use part a to prove the equivalence in 3d on Set 1 holds for integer-valued polynomials.