Practice Problems

The following problems are intended as practice in preparation for the Test scheduled for Monday, April 7 during class time (7:30–8:50 am). The content covered is outlined on a separate review sheet posted on the course website (roughly the content covered prior to Spring Break). The actual test will consist of four questions similar in structure to #1–11 below (together worth at least 70%); plus ten true-false questions similar to #12 below (together worth 30%). By indicating 'at least 70%', I allow the possibility of bonus points.

Instructions: Closed book; however, a 'cheat sheet' (one $8\frac{1}{2}'' \times 11''$ sheet with your own handwriting) and a calculator are permitted. Cell phones may not be used (in particular they cannot serve as calculators during this test). *Clarity is required for full credit*. Time allowed: 50 minutes. Total value of questions: 100 points.

1. Let $n = 2025$.
   (a) How many divisors does n have? List them all.
   (b) Evaluate $\phi(n)$.
   (c) Using Euclid's Algorithm, evaluate $d = \gcd(81, n)$ and find integers r, s such that $81r + ns = d$.
   (d) Is the solution (r, s) in (c) unique? What are *all* integer solutions of the equation $81r + ns = d$?

2. Find *all* integer solutions of
$$x \equiv 6 \mod 13 \quad \text{and} \quad x \equiv 5 \mod 11.$$

3. Let $n = pq$ where p and q are large primes. Assume that the explicit value of n is given, but that the factors p and q are not explicitly given. Show that if the explicit value of $\phi(n)$ is also given, then one has enough information to easily factor n (i.e. to determine the factors p and q). Here ϕ is Euler's totient function.

4. Does every Pythagorean triple have the form $(m^2-n^2, 2mn, m^2+n^2)$ for some integers m, n? Justify your answer.

5. You are given 20-digit natural numbers m, p, r where p is prime and $\gcd(m, p-1) = 1$. Explain how to find an integer g satisfying $g^m \equiv r \mod p$.

6. In our proof of Fermat's Little Theorem, we used the product of the nonzero elements of the field $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ (although our proof did not require knowing the explicit value of this product). Prove that this product is actually equal to $-1 \in \mathbb{F}_p$.

7. Given that $n = a^2 + b^2$ for some integers a, b, find integers c, d such that $26n = c^2 + d^2$.

8. Show that $a^{1104} \equiv 1 \mod 1105$ whenever $\gcd(a, 1105) = 1$. You may use the prime factorization $1105 = 5 \cdot 13 \cdot 17$.

9. Find all solutions of $n = 2\phi(n)$, where ϕ is Euler's totient function. Justify your answer.

10. Let $f(x)$ be a non-constant polynomial in x with integer coefficients. Is it possible for $f(n)$ to be prime for every positive integer n? Justify your answer.

11. Consider an integer $p \geqslant 2$. If $a^{p-1} \equiv 1 \mod p$ for every $a \in \{1, 2, 3, \ldots, p-1\}$, does it necessarily follow that p is prime? Justify your answer.

12. Answer TRUE or FALSE to each of the following statements.

    (a) The equation $x^3 + y^3 = z^3$ has infinitely many solutions in positive integers. _____*(True/False)*

    (b) Fermat's Little Theorem is the main tool available to factor large integers. _____*(True/False)*

    (c) There are infinitely many primes of the form $N^2 - 1$. _____*(True/False)*

    (d) If the numbers $p_1, p_2, , p_k$ are distinct primes, then necessarily the number $N = 4p_1p_2 \cdots p_k - 1$ is prime. _____*(True/False)*

    (e) Goldbach proved that every even integer $2n \geqslant 4$ has the form $2n = p + q$ for some primes p, q (not necessarily distinct). _____*(True/False)*

    (f) If an integer n divides ab, then either n divides a, or n divides b. _____*(True/False)*

    (g) If m and n are relatively prime positive integers whose product is a perfect square, then both m and n must be perfect squares. _____*(True/False)*

(h) The equation $x^2 - 19y^2 = 1$ has infinitely many integer solutions.
_____*(True/False)*

(i) There are infinitely many primes p such that $p^2 + 1$ is prime. _____*(True/False)*

(j) If $ra + sb = 2$ for some integers r, s, a, b, then necessarily $\gcd(a, b) = 2$.
_____*(True/False)*