Math 661
Algebraic Number Theory
Problem Set 1

(1) Modify Euclid's proof of the infinitude of primes to show that there are infinitely many primes congruent to 3 mod 4. (Hint: Suppose there are only a finite number of such primes, say $q_1, \ldots, q_k$. What is their product congruent to mod 4? Consider $n = q_1 \cdots q_k + 2$ if k is even, or $n = q_1 \cdots q_k + 4$ if k is odd. Study the primes that divide n. In Problem 4 below, we will show that there are infinitely many primes congruent to 1 mod 4 as well.)

(2) We will prove in this problem that any finite subgroup G of the multiplicative group of a field F is cyclic. In particular, this shows that the group $\mathbb{F}_q^*$ is cyclic for any finite field $\mathbb{F}_q$. There are many proofs, and they all use the fact that over a field, the equation $x^t - 1 = 0$ has at most t solutions. Here is one proof that studies p-Sylow subgroups of G. Let $|G| = n$.
   (a) Let p be a prime divisor of n. Let k be the maximum of the set $\{l \mid \exists\ h \in G$ with order of $h = p^l\}$. Let g be an element of order p^k. Show that if h is any element of G of order p^l for some l, then $h \in \langle g \rangle$. (Hint: use the fact alluded to above: $x^t - 1 = 0$ has at most t solutions in F.)
   (b) Conclude that for any p that divides n, there is a unique p-Sylow subgroup of G, and it is cyclic.
   (c) Conclude using the Chinese Remainder Theorem that G is cyclic.

(3) Let p be an odd prime. Show that $x^2 + 1 \equiv 0 \bmod p$ has a solution in $\mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$. (This is often referred to as "-1 is a square mod p" if and only if $p \equiv 1 \bmod 4$. Hint: Use the result of Problem 2 above.)

(4) Show that there are infinitely many primes congruent to 1 mod 4. (Hint: Assume there are only finitely many such, $q_1, \ldots, q_k$. As in Problem 1, consider some suitable product of these primes, but in such a way that the result of Problem 3 will be violated.)

(5) Prove Wilson's theorem: p is prime if and only if $(p-1)! + 1 \equiv 0 \bmod p$. (Hint: If p is prime, recall that the group $\mathbb{F}_p^*$ is cyclic, by Problem 2 above. View the product $(p-1)! \bmod n$ as the product of all the elements of the group $\mathbb{F}_p^*$. Study cancellations in this product. For the converse, if p is composite, say $p = ab$ where a and b are greater than 1, what can you say about a and b in relation to $(p-1)! = (ab-1)!$?)

(6) Recall the definition of the *Fermat numbers:* $F_n := 2^{2^n} + 1$, $n = 0, 1, \ldots$. (Recall the convention about repeated exponents: 2^{2^n} stands for 2 raised to the power 2^n—as opposed to 2^2 raised to the power n.) Thus, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, and so on. (Fermat conjectured that the F_n are all prime. However, while F_0 through F_4 are all prime, Euler showed that F_5, a ten-digit number, is not prime: it is divisible by 641. It is an open question if there are infinitely many Fermat numbers that are prime. In fact, it is an open question where F_n is prime for *any* $n > 5$.) Show that if $n \neq m$, then F_n and F_m are relatively prime, and use this result to give another proof that there are infinitely many prime numbers. (Hint: Say $n > m$. If a prime p divides F_m, show that it must divide $F_n - 2$.)

(7) We will provide a bound on the size of the k-th prime in this exercise using just unique prime factorization. In what follows, p_k with denote the k-th prime, $k = 1, 2, \ldots$.
   (a) Show that $p_{k+1} \leq p_1 \cdot p_2 \cdots p_k + 1$. (Hint: Use the same sort of arguments as in Euclid's proof of the infinitude of primes.)
   (b) Use induction and the result in Part 7a above to show that $p_k < 2^{2^k}$. (Remark: Incidentally, much tighter bounds can be found with a little more work: for instance, $p_k < 6k(2\log k + 2\log\frac{12}{e})$ — see Apostol's Introduction to Analytic Number Theory. The ultimate prize in this direction is the Prime Number Theorem, which states that $\pi(x) \sim \frac{x}{\log x}$, where $\pi(x)$ is the number of primes less than or equal to x, and $\sim$ means that the two quantities on either side have ratio 1 as $x \to \infty$.)

(8) Smallest prime factor of an integer n:
   (a) Show that if n is composite, then its smallest prime factor is bounded above by $\sqrt{n}$.
   (b) Show that if the smallest prime factor of an integer n (> 1) exceeds $\sqrt[3]{n}$ then n must either be prime or have just two prime factors.

(9) We will solve an old familiar equation in this problem! We will show that every solution in integers of the equation $x^2 + y^2 = z^2$, where x, y, and z have no common factor, is of the form $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, for some relatively prime integers m and n, not both odd. (Recall that triples of integers (x, y, z) satisfying $x^2 + y^2 = z^2$ are called *Pythagorean triples,* and Pythagorean triples satisfying the additional condition of not having a common factor are called *primitive* Pythagorean triples.)
   (a) Verify that if m and n are relative prime integers, not both odd, then $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$ forms a primitive Pythagorean triple.
   (b) Now for the converse (in several steps!). Suppose that (x, y, z) is a primitive Pythagorean triple. Note that $z \neq 0$ (why?). Show that $\frac{x}{z} = \cos(\theta)$ and $\frac{y}{z} = \sin(\theta)$ for suitable θ with $0 \leq \theta < 2\pi$.
   (c) Let $t = \tan(\theta/2)$. Show that $\frac{x}{z} = \frac{1 - t^2}{1 + t^2}$ and $\frac{y}{z} = \frac{2t}{1 + t^2}$. (Hint: Just invoke an identity from trigonometry.)
   (d) Show that t must be a rational number.
   (e) Write $t = \frac{n}{m}$ where m and n are relatively prime integers. Use Parts 9c and 9d, along with the fact that x, y, and z have no common factor to show that x must equal $m^2 - n^2$, y must equal $2mn$, and z must equal $m^2 + n^2$. Use the fact that x, y, and z have no common factor to argue that m and n cannot both be odd.

   Remark: Given that $x^2 + y^2 = z^2$, the condition that x, y, and z share no common factor is equivalent to the condition that any two of x, y, and x must be relatively prime . (Think about this!)

(10) We will solve the $n = 4$ case of Fermat's Last Theorem: There are no pairwise relatively prime integer solutions to $x^4 + y^4 = z^4$. We will use a method now called Fermat Descent: assume there is a solution with a given (positive) value of z, and show that there must be another solution with a

smaller positive value of z. Since this process cannot go on indefinitely, we have a contradiction, and there cannot be any solutions.

(a) Write w for z^2, so that we are solving $x^4 + y^4 = w^2$ for pairwise relatively prime integers. Assume there is a solution (X, Y, W) to this equation, where we can assume without loss of generality that W is positive. Show that there must exist relatively prime integers m and n, not both odd, such that $X^2 = m^2 - n^2$, $Y^2 = 2mn$, and $W = m^2 + n^2$.

(b) Now show that there must exist relatively prime integers r and s, not both odd, such that $X = r^2 - s^2$, $n = 2rs$, and $m = r^2 + s^2$.

(c) Show that r, s, and m are pairwise relatively prime. Use this and the fact that $Y^2 = 4rsm$ to conclude that $r = A^2$, $s = B^2$, and $m = C^2$ for some integers A, B, and C, where C may be assumed positive.

(d) Show that we get another pairwise relatively prime solution (A, B, C) to $x^4 + y^4 = w^2$ with $0 < C < W$. Argue that this proves that there are no pairwise relatively prime integers solutions to $x^4 + y^4 = z^4$.