MTH 505: Number Theory **Spring 2020**
Homework 2 **Drew Armstrong**

Problem 1. Smith Normal Form. Find unimodular matrices U and V satisfying

$$V\begin{pmatrix}7 & 5 & 3\\ 6 & 4 & 2\end{pmatrix}U=\begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 0\end{pmatrix}.$$

Use your answer from part (a) to solve the following system of Diophantine equations:

$$\begin{cases} 7x_1 + 5x_2 + 3x_3 = 1,\\ 6x_1 + 4x_2 + 2x_3 = 0.\end{cases}$$

Problem 2. Modular Arithmetic is Well-Defined. For all integers $a, b, a', b' \in \mathbb{Z}$ with $a \equiv a'$ and $b \equiv b' \bmod n$, show that $a+b \equiv a'+b$ and $ab \equiv a'b' \bmod n$.

Problem 3. Irrational Roots. Let $d, n \in \mathbb{Z}$ be positive integers and let $\sqrt[n]{d} \in \mathbb{R}$ denote the positive real nth root. We will show that $\sqrt[n]{d} \notin \mathbb{Z}$ implies $\sqrt[n]{d} \notin \mathbb{Q}$.

(a) Assume that $\sqrt[n]{d} \notin \mathbb{Z}$ and for each prime p let $\nu_p(d) \in \mathbb{N}$ denote the multiplicity of p in the factorization of d. Prove that there exists some prime p with $\nu_p(d) \not\equiv 0 \bmod n$.

(b) Now assume for contradiction that $\sqrt[n]{d} \in \mathbb{Q}$. This means we can write $(a/b)^n = d$, and hence $a^n = db^n$, for some integers $a, b \in \mathbb{Z}$ with $b \neq 0$. Prove that $n\nu_p(a) = \nu_p(d) + n\nu_p(b)$ and explain why this contradicts part (a).

Problem 4 Infinitely Many Primes $\equiv 3$ Mod 4. We will show that there are infinitely many prime numbers in the sequence $\{3+4k : k \in \mathbb{Z}, k \geqslant 0\}$.

(a) For any positiver integer n with $n \equiv 3 \bmod 4$, show that n has a prime factor $p|n$ satisfying $p \equiv 3 \bmod 4$. [Hint: If not then every prime factor of n is $\equiv 1 \bmod 4$.]

(b) Assume for contradiction that there are finitely many primes $\equiv 3 \bmod 4$ and call them

$$3 < p_1 < p_2 < \cdots < p_k.$$

Now consider the number $n = 4p_1p_2\cdots p_k + 3$. From part (a) there exists a prime factor $p|n$ with $p \equiv 3 \bmod 4$. Show that this prime is not in the list.

Problem 5. RSA Cryptosystem. We will fill in a gap from our in-class discussion of RSA.

(a) For all integers $p, q, a \in \mathbb{Z}$ with $\gcd(p,q) = 1$ show that $p|a$ and $q|a$ imply $pq|a$. [Hint: By Bézout we can write $px + qy = 1$ for some $x, y \in \mathbb{Z}$. Now multiply both sides by a.]

(b) For any integers $m, k, p, q \in \mathbb{Z}$ with p and q prime, show that

$$p|m(m^{\phi(p)\phi(q)k} - 1) \quad \text{and} \quad q|m(m^{\phi(p)\phi(q)k} - 1).$$

[Hint: If $p \nmid m$ then Euler's Totient Theorem says that $m^{\phi(p)} \equiv 1 \bmod p$. Similarly, if $q \nmid m$ then we have $m^{\phi(q)} \equiv 1 \bmod q$.]

(c) If p and q are distinct primes, combine parts (a) and (b) to show that

$$m^{\phi(p)\phi(q)k+1} \equiv m \bmod pq$$

for all integers $m, k \in \mathbb{Z}$.

Problem 6. Infinitely Many Primes $\equiv$ 1 Mod 4. We will show that there are infinitely many prime numbers in the sequence $\{1 + 4k : k \in \mathbb{Z}, k \geqslant 0\}$.

(a) Assume for contradiction that there are only finitely many primes in this sequence; call them $p_1, p_2, \ldots, p_k$ and define the integers

$$x = 2p_1p_2 \cdots p_k \quad \text{and} \quad n = x^2 + 1.$$

Prove that $n \equiv 1 \bmod 4$ and $n \equiv 1 \bmod p_i$ for all i.

(b) Let $p|n$ be any prime divisor of n. Show that $x, x^2, x^3 \not\equiv 1$ and $x^4 \equiv 1 \bmod p$. It follows from Euler's Totient Theorem that 4 divides $\phi(p) = p - 1$ and hence $p \equiv 1 \bmod 4$. But then we must have $p = p_i$ for some i. Show that this leads to a contradiction.