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 to solve the following system of Diophantine equations:

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

There are infinitely many such matrices U and V, depending on the particular sequence of row and column operations. Here is one such sequence:

$$\begin{array}{ccc|cc} 7 & 5 & 3 & 1 & 0 \\ 6 & 4 & 2 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array} \quad\rightsquigarrow\quad \begin{array}{ccc|cc} 3 & 5 & 7 & 1 & 0 \\ 2 & 4 & 6 & 0 & 1 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & 0 & 0 & & \end{array} \quad\rightsquigarrow\quad \begin{array}{ccc|cc} 2 & 4 & 6 & 0 & 1 \\ 3 & 5 & 7 & 1 & 0 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & 0 & 0 & & \end{array}$$

$$\rightsquigarrow\quad \begin{array}{ccc|cc} 2 & 0 & 0 & 0 & 1 \\ 3 & -1 & -2 & 1 & 0 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & -2 & -3 & & \end{array} \quad\rightsquigarrow\quad \begin{array}{ccc|cc} 2 & 0 & 0 & 0 & 1 \\ 1 & -1 & -2 & 1 & -1 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & -2 & -3 & & \end{array} \quad\rightsquigarrow\quad \begin{array}{ccc|cc} 1 & -1 & -2 & 1 & -1 \\ 2 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & -2 & -3 & & \end{array}$$

$$\rightsquigarrow\quad \begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1 \\ 2 & 2 & 4 & 0 & 1 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & -1 & -1 & & \end{array} \quad\rightsquigarrow\quad \begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1 \\ 0 & 2 & 4 & -2 & 3 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & -1 & -1 & & \end{array} \quad\rightsquigarrow\quad \begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1 \\ 0 & 2 & 0 & -2 & 3 \\ \hline 0 & 0 & 1 & & \\ 0 & 1 & -2 & & \\ 1 & -1 & 1 & & \end{array}$$

From this we conclude that

$$VAU = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}\begin{pmatrix} 7 & 5 & 3 \\ 6 & 4 & 2 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -2 \\ 1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = D.$$

Now we want to find all integer vectors $\mathbf{x}$ such that $A\mathbf{x} = \mathbf{b}$, where $\mathbf{b} = (1, 0)$. By setting $\mathbf{y} = U^{-1}\mathbf{x}$, this is equalent to

$$\begin{aligned} A\mathbf{x} &= \mathbf{b} \\ V^{-1}DU^{-1}\mathbf{x} &= \mathbf{b} \\ DU^{-1}\mathbf{x} &= V\mathbf{b} \\ D\mathbf{y} &= V\mathbf{b} \end{aligned}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} y_1 \\ 2y_2 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \end{pmatrix}.$$

The complete integer solution is $(y_1, y_2, y_3) = (1, -1, k)$ for all $k \in \mathbb{Z}$, and hence

$$\begin{aligned}
\mathbf{x} &= U\mathbf{y} \\
\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -2 \\ 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ k \end{pmatrix} \\
\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= 1 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - 1 \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} + k \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \\
\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix} + k \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \qquad \text{for all } k \in \mathbb{Z}.
\end{aligned}$$

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

Proof. Assume that we have $a \equiv a'$ and $b \equiv b'$ mod n. By definition this means that $a - a' = nk$ and $b - b' = n\ell$ for some integers $k, \ell \in \mathbb{Z}$. But then we have

$$(a + b) - (a' + b') = (a - a') + (b - b') = nk + n\ell = n(k + \ell),$$

which implies that $a + b \equiv a' + b'$ mod n and

$$\begin{aligned}
ab - a'b' &= (a' + nk)(b' + n\ell) - a'b' \\
&= a'b' + b'nk + a'n\ell + n^2k\ell - a'b' \\
&= n(b'k + a'\ell + nk\ell),
\end{aligned}$$

which implies that $ab \equiv a'b'$ mod n. $\square$

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 $\nu_p(d) \not\equiv 0$ mod 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).

(a): If not, then for each prime p_i we can write $\nu_{p_i}(d) = nk_i$ for some $k_i \in \mathbb{Z}$. It follows that

$$\begin{aligned}
d &= p_1^{\nu_{p_1}(d)} p_2^{\nu_{p_2}(d)} p_3^{\nu_{p_3}(d)} \cdots \\
&= p_1^{nk_1} p_2^{nk_2} p_3^{nk_3} \cdots \\
&= \left(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots\right)^n,
\end{aligned}$$

which contradicts the fact that $\sqrt[n]{d} \notin \mathbb{Z}$.

(b) Assume that $(a/b)^n = d$ for some integers $a, b \in \mathbb{Z}$ with $b \neq 0$. Then raising both sides to the power of n and multiplying by b^n gives $a^n = db^n$. From part (a) we know there exists a prime p such that $n \nmid \nu_p(d)$. But recall that the function $\nu_p : \mathbb{Z} \to \mathbb{N}$ satisfies $\nu_p(xy) = \nu_p(x) + \nu_p(y)$. Thus we obtain the following contradiction:

$$\begin{aligned} a^n &= db^n \\ \nu_p(a^n) &= \nu_p(db^n) \\ n\nu_p(a) &= \nu_p(d) + n\nu_p(b) \\ n(\nu_p(a) - \nu_p(b)) &= \nu_p(d). \end{aligned}$$

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.

(a): Let $n \equiv 3 \bmod 4$. We can express $n = q_1 \cdots q_k$ as a product of primes, and since n is odd we know that the prime 2 does not occur. Thus for each i we have $q_i \equiv 1$ or $q_i \equiv 3 \bmod 4$. If $q_i \equiv 1 \bmod 4$ for all i then we obtain a contradiction:

$$n \equiv q_1q_2 \cdots q_k \equiv 1 \cdot 1 \cdots 1 \equiv 1 \bmod 4.$$

Therefore there must exist some i such that $q_i \equiv 3 \bmod 4$.

(b): Assume for contradiction that $3 < p_1 < p_2 < \cdots < p_k$ are the only primes $\equiv 3 \bmod 4$ and define the number $n = 3 + 4p_1 \cdots p_k$. Since $n \equiv 3 + 0 \equiv 3 \bmod 4$ we know from part (a) that there exists some prime $p|n$ with $p \equiv 3 \bmod 4$. But I claim that this p is not in the list $3, p_1, \ldots, p_k$. Indeed, if $p = 3$ then we see that 3 divides $n - 3 = 4p_1 \cdots p_k$, which by Euclid's Lemma implies that $3|4$ or $3|p_i$ for some i. But this is impossible because $p_i \neq 3$ and p_i is prime. And if $p = p_i$ for some i then we see that p_i divides $n - 4p_1 \cdots p_k = 3$, which is impossible because $3 < p_i$. Therefore our list was incomplete. $\square$

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 $m, k \in \mathbb{Z}$.

(a): Let $p, q, a \in \mathbb{Z}$ with $\gcd(p, q) = 1$. Then from Bézout's Identity we can write $px + qy = 1$ for some $x, y \in \mathbb{Z}$. Now suppose that we have $p|a$ and $q|a$ for some $a \in \mathbb{Z}$. Say $a = pk$ and $a = q\ell$. It follows that

$$\begin{aligned} px + qy &= 1 \\ a(px + qy) &= a \\ apx + aqy &= a \\ q\ell px + pkqy &= a \\ pq(\ell x + ky) &= a, \end{aligned}$$

and hence $pq|a$.

(b): Let $m, k, p, q \in \mathbb{Z}$ with p, q prime. If $p \nmid m$ then Euler's Totient Theorem implies that

$$\begin{aligned} m^{\phi(p)} &\equiv 1 \\ (m^{\phi(p)})^{\phi(q)k} &\equiv 1^{\phi(q)k} \\ m^{\phi(p)\phi(q)k} &\equiv 1 \bmod pq. \end{aligned}$$

This implies that pq (and also p) divides $m^{\phi(p)\phi(q)k} - 1$, and hence p divides $m(m^{\phi(p)\phi(q)k} - 1)$. But if $p|m$ then we still have $p|m(m^{\phi(p)\phi(q)k} - 1)$. The same result for q follows by symmetry.

(c): Finally, if $p \neq q$ then we have $\gcd(p, q) = 1$ and it follows from part (a) that

$$pq|m(m^{\phi(p)\phi(q)k} - 1) = m^{\phi(p)\phi(q)k+1} - m.$$

In other words, we have $m^{\phi(p)\phi(q)k+1} \equiv m \bmod pq$. This formula is the basis for decryption in the RSA cryptosystem.

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.

(a): Assume for contradiction that $p_1, \ldots, p_k$ are the only primes $\equiv 1 \bmod 4$, and define

$$\begin{aligned} x &= 2p_1 \cdots p_k, \\ n &= x^2 + 1. \end{aligned}$$

Since $4|x^2 = n-1$ we have $n \equiv 1 \bmod 4$ and since $p_i|x^2 = n-1$ we have $n \equiv 1 \bmod p_i$ for all indices i.

(b): We know that n has some prime divisor $p|n$. If we can show that

(1) p is not in the list $p_1, \ldots, p_k$,

(2) $p \equiv 1 \bmod 4$,

then we will obtain the desired contradiction. To show (1), suppose that $p = p_i$ for some i. Then we obtain the contradiction $p_i|(n-x^2) = 1$. To show (2), it is enough to prove that $x \not\equiv 0$, $x, x^2, x^3 \not\equiv 1$ and $x^4 \equiv 1 \bmod 4$. In other words, it is enough to show that $4 = \mathsf{ord}_p(x)$ is the multiplicative order of x mod p. Then Euler's Totient Theorem will imply that $4 = \mathsf{ord}_p(x)|\phi(p) = p-1$ and hence $p \equiv 1 \bmod 4$.

To do this we first observe that $p|n = x^2+1 = x^2-(-1)$. This implies that $x^2 \equiv -1$ and hence $x^4 \equiv (x^2)^2 \equiv (-1)^2 \equiv 1 \bmod p$. Then since $p|n$ and n is odd we know that $p \neq 2$, which implies that $x \equiv -1 \not\equiv 1 \bmod p$. It follows that $x \not\equiv 0$ and $x \not\equiv 1 \bmod 4$ since otherwise squaring both sides would give the contradictions $x^2 \equiv 0$ and $x^2 \equiv 1 \bmod 4$. Finally, we observe that $x^3 \equiv 1 \bmod 4$ is impossible since multiplying by x would give the contradiction $x \equiv x^4 \equiv 1 \bmod 4$. $\square$

Discussion: The proof given here can be generalized to show that there are infinitely many primes $\equiv 1 \bmod n$ for any integer $n \geqslant 2$. The general idea is to replace the expression x^2+1 by a certain polynomial $\Phi_n(x)$, called the *cyclotomic polynomial.* It is also true that for any $\gcd(a,b) = 1$ there exist infinitely many primes $\equiv a \bmod b$. This is a famous theorem called Dirichlet's Theorem and it is extremely difficult to prove.