Homework 4

Chris Powell

A. Let $d \mid a$, $d \mid b$. Show that

$$\gcd(a, b) = d \gcd\left(\frac{a}{d}, \frac{b}{d}\right).$$

Proof. As $d \mid a, b$, we know $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. By the Linear Equation Theorem, we know that $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$. Likewise, there exists $s, t \in \mathbb{Z}$ such that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{a}{d}s + \frac{a}{d}t$. Note that $\gcd(a, b)$ and $\gcd\left(\frac{a}{d}, \frac{b}{d}\right)$ are the least postive values of $ax + by$ and $\frac{a}{d}s + \frac{b}{d}t$, respectively. Thus

$$d \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = d\left(\frac{a}{d}s + \frac{b}{d}t\right) = as + bt \geqslant ax + by = \gcd(a, b).$$

On the other hand,

$$d \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = d\left(\frac{a}{d}s + \frac{b}{d}t\right) \leqslant d\left(\frac{a}{d}x + \frac{b}{d}y\right) = ax + by = \gcd(a, b).$$

Hence $\gcd(a, b) = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$. □

B. Silverman 7.3. Let s and t be odd integers with $s > t \geqslant 1$ and $\gcd(s, t) = 1$. Prove that the three numbers

$$st, \quad \frac{s^2 - t^2}{2}, \quad \text{and} \quad \frac{s^2 + t^2}{2}$$

are pairwise relatively prime.

Proof. Since $\left(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}\right)$ is a primitive Pythagorean triple, it suffices to show that $g = \gcd\left(st, \frac{s^2-t^2}{2}\right) = 1$, as any pairwise common divisor must be a common divisor of the other pairs. Suppose otherwise that $g > 1$. Then by the Fundamental Theorem of Arithmetic, there exists a prime factor p of g. Thus $p \mid st, \frac{s^2-t^2}{2}$ by transitivity of the divisibility relation. Therefore either $p \mid s$ or $p \mid t$ since p is prime. Suppose $p \mid s$. Since $p \mid \frac{s^2-t^2}{2}$, we have that $\frac{s^2-t^2}{2} = pk$ for some $k \in \mathbb{Z}$. Thus

$$2pk = s^2 - t^2 = (s+t)(s-t).$$

So $p \mid (s+t)(s-t)$ which implies that either $p \mid s+t$ or $p \mid s-t$. Either way, this implies $p \mid t$. So $p \mid s, t$. But $\gcd(s,t) = 1$, a contradiction. A similar argument holds if $p \mid t$. □

C. Recall that for $n \in \mathbb{N}$, $n!$ means $n \cdot (n-1) \cdots 2 \cdot 1$. How many 0s does 100! end in?

Note that $100! = 100 \cdot 99 \cdots 2 \cdot 1$. A trailing 0 is formed from the product of a multiple of some power of 5 and a multiple of some power of 2. So we add the powers of 5 which divide 100:

$$\sum_{k:5^k \mid 100} \frac{100}{5^k} = \frac{100}{5^1} + \frac{100}{5^2} = \frac{100}{5} + \frac{100}{25} = 20 + 4 = 24.$$

Since there are clearly more multiples of 2 than 5 in $\{1, \ldots, 100\}$, we conlude that there are 24 trailing zeros in 100!.

D. Let $n \in \mathbb{N}$ have prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where the p_i are distinct primes and the $e_i \geqslant 1$. Show that n is a perfect square if, and only if, $2 \mid e_i$ for all i.

Proof. Suppose n is a perfect square. Then $n = m^2$ for some $m \in \mathbb{Z}$. By the Fundamental Theorem of Arithmetic, m has a unique prime factorization $m = \prod_{i=1}^{s} q_i^{d_i}$, where each d_i is distinct. Since this factorization is unique (up to rearrangment), we know that $r = s$ and that there is some permutation σ such that $p_i = \sigma(q_i)$ for all $i \in \{1, \ldots, r\}$. Hence

$$n = \left(\prod_{i=1}^{s} q_i^{d_i}\right)^2 = \prod_{i=1}^{s} \left(q_i^{d_i}\right)^2 = \prod_{i=1}^{s} q_i^{2d_i}.$$

By uniqueness, $e_i = 2d_i$ for all i. Thus $2 \mid e_i$ for all i. Conversely, if $2 \mid e_i$ for all i, then

$$n = \prod_{i=1}^{r} p_i^{2d_i} = \prod_{i=1}^{r} (p_i^{e_i})^2 = \left(\prod_{i=1}^{r} p_i^{e_i}\right)^2.$$

Since $\mathbb{Z}$ is closed under multiplication, $n = m^2$ for some $m \in \mathbb{Z}$. □

E. Silverman 8.5 Find all incongruent solutions to each of the following linear congruences.

(a) $8x \equiv 6 \pmod{14}$

First, we apply the Euclidean algorithm to evaluate $g = \gcd(8, 14)$:

$$\begin{aligned} 14 &= 1(8) + 6 \quad (q_1, r_1) = (1, 6) \\ 8 &= 1(6) + 2 \quad (q_2, r_2) = (1, 2) \\ 6 &= 3(2) + 0 \quad (q_3, r_3) = (3, 0). \end{aligned}$$

Since $r_3 = 0$, it follows that $g = r_2 = 2$. Since $2 \mid 14$, the Linear Congruence Theorem implies that $8x \equiv 6 \pmod{14}$ has exactly 2 incongruent solutions. By the Linear Equation Theorem, we can find $u, v \in \mathbb{Z}$ which satisfy

$$8u + 14v = 2. \quad (*)$$

Write $a = 14$ and $b = 8$. Then

$$\begin{aligned} r_1 &= a - q_1 b \\ &= a - (1)b \\ r_2 &= b - q_2 r_1 \\ &= b - (1)(a - (1)b) \\ &= (-1)a + 2b \end{aligned}$$

Thus $(u, v) = (2, -1)$ is a solution to $(*)$. So $3 \cdot (u, v) = (6, -3)$ is a solution to

$$8u + 14v = 6. \quad (**)$$

Therefore, by the Linear Congruence Theorem, $x = 6\frac{u}{g} = 6$ is a solution to $8x \equiv 6 \pmod{14}$, and the set of all incongruent solutions is given by $x \equiv 6 + 7k$ for all $k \in \{0, 1\}$. Explicitly, this yields $x \equiv 6 \pmod{14}$ and $x \equiv 13 \pmod{14}$.

(b) $66x \equiv 100 \pmod{121}$

First, we apply the Euclidean algorithm to evaluate $\gcd(66, 121)$:

$$\begin{aligned} 121 &= 1(66) + 55 \quad (q_1, r_1) = (1, 55) \\ 66 &= 1(55) + 11 \quad (q_2, r_2) = (1, 11) \\ 55 &= 5(11) + 0 \quad (q_3, r_3) = (5, 0). \end{aligned}$$

Since $r_3 = 0$, we know $\gcd(66, 121) = r_2 = 11$. But since $11 \nmid 100$, the Linear Congruence Theorem implies that $66x \equiv 100 \pmod{121}$ has no solutions, i.e.,

$$\{x \in \mathbb{Z} \mid 66x \equiv 100 \pmod{121}\} = \varnothing.$$

(c) $21x \equiv 14 \pmod{91}$

We first apply the Euclidean algorithm to evaluate $g = \gcd(21, 91)$:

$$\begin{aligned} 91 &= 4(21) + 7 \quad (q_1, r_1) = (4, 7) \\ 21 &= 3(7) + 0 \quad (q_2, r_2) = (1, 2) \end{aligned}$$

Since $r_2 = 0$, we know $g = r_1 = 7$. Since $7 \mid 14$, the Linear Congruence Theorem implies that $21x \equiv 14 \pmod{91}$ has exactly 7 incongruent solutions. By the Linear Equation Theorem, we know there exists $u, v \in \mathbb{Z}$ satisfying

$$21u + 91v = 7. \quad (*)$$

Write $a = 91$ and $b = 21$. Then

$$\begin{aligned} r_1 &= a - q_1 b \\ &= a - (4)b \end{aligned}$$

Thus $(u, v) = (-4, 1)$ is a solution to $(*)$. So $2 \cdot (u, v) = (-8, 2)$ is a solution to

$$21u + 91v = 14. \quad (**)$$

Therefore, by the Linear Congruence Theorem, $x = 14\frac{u}{g} = -8$ is a solution to $21x \equiv 14 \pmod{91}$, and the set of all incongruent solutions is given by $x \equiv -8 + (13)k$ for all $k \in \{0, \ldots, 6\}$. Explicitly, this yields incongruent solutions [5], [18], [31], [44], [57], [70], and [83].

F. Silverman 8.6 Determine the number of incongruent solutions for each of the following congruences. You do not need to write down the actual solutions.

(a) $72x \equiv 47 \pmod{200}$

We first apply the Euclidean algorithm to evaluate $g = \gcd(72, 200)$:

$$\begin{aligned} 200 &= 2(72) + 56 \quad (q_1, r_1) = (2, 56) \\ 72 &= 1(56) + 16 \quad (q_2, r_2) = (1, 16) \\ 56 &= 3(16) + 8 \quad (q_3, r_3) = (3, 8) \\ 16 &= 2(8) + 0 \quad (q_4, r_4) = (2, 8) \end{aligned}$$

Since $r_4 = 0$, we have that $\gcd(72, 200) = r_3 = 8$. But since $8 \nmid 47$, the Linear Congruence Theorem implies that $72x \equiv 47 \pmod{200}$ has no soluitions, i.e.,

$$\{x \in \mathbb{Z} \mid 72x \equiv 47 \pmod{200}\} = \varnothing.$$

(b) $4183x \equiv 5781 \pmod{15087}$

Since $\gcd(4183, 15087) = 47 \mid 5781$, the Linear Congruence Theorem implies that $4183x \equiv 5781 \pmod{15087}$ has 47 incongruent solutions.

(c) $1537x \equiv 2863 \pmod{6731}$

Since $\gcd(1537, 6731) = 53 \nmid 2863$, the Linear Congruence Theorem implies that $1537x \equiv 2863 \pmod{6731}$ has no solution, i.e.,

$$\{x \in \mathbb{Z} \mid 1537x \equiv 2863 \pmod{6731}\} = \varnothing.$$

G. Silverman 8.7 Write a program that solves the congruence

$$ax \equiv c \pmod{m}.$$

```
def xgcd(a, b):
    """Return (g, x, y) such that a*x + b*y = g = gcd(a, b)"""
    if b == 0:
        return a, 1, 0
    x, g, v, w = 1, a, 0, b
    while w != 0:
        x, g, v, w = v, w, x - (g // w) * v, g % w
    x = x % (b // g)
    y = (g - (a * x)) // b
    return g, x, y


def cong(a, c, m):
    """Return {x in Z | ax = c (mod m)}"""
    g = xgcd(a, m)[0]
    S = []
    if c % g != 0:
        return S  # solution-set S is empty
    else:
        x = (c * xgcd(a, m)[1]) // g
        for i in range(0, g):
            S = S + [(x + i * (m // g)) % m]
    return S  # return g incongruent solutions
```