Number Theory – HW 2 – Due September 26

Problem 1 (a) *Suppose that $\mathcal{S}$ contains $2n$ elements and that $\mathcal{S}$ is partitioned into n disjoint subsets, each one containing exactly two of its elements. Show that this can be done in precisely*

$$(2n-1)(2n-3)\dots 5\cdot 3\cdot 1 = \frac{(2n)!}{2^n n!}$$

ways.

(b) *Show that $(n+1)(n+2)\dots(2n)$ is divisible by 2^n, but not by 2^{n+1}.*

Solution.

a. *Consider a set A with $n \in \mathbb{N}$ elements, for an even n. Let us find a recursive expression for the number of partitions, each of which only containing two elements. Let $P(n)$ be the number of ways we may form such partitions in a finite set of n elements. Consider an arbitrary element $k \in A$. There are $(n-1)$ ways k can be paired with another element, and $P(n-2)$ ways the remaining $n-2$ elements can be partitioned into sets of 2. So we write*

$$P(n) = (n-1)\cdot P(n-2)$$

Clearly, there is one way to form a partition with only 2 elements so

$$P(2) = 1.$$

Now $|\mathscr{S}| = 2n$, so the number of ways we can partition $\mathscr{S}$ into sets of cardinality 2 is

$$\begin{aligned}
P(2n) &= (2n-1)P(2n-2)\\
&= (2n-1)(2n-3)P(2n-4)\\
&\dots\\
&= (2n-1)(2n-3)\cdots 5\cdot 3\cdot P(2)\\
&= (2n-1)(2n-3)\cdots 5\cdot 3\cdot 1
\end{aligned}$$

We note that

$$\begin{aligned}
(2n)(2n-1)(2n-2)\cdots(2)(1) &= (2n)!\\
[(2n-1)(2n-3)\cdots(5)(3)(1)]\,[(2n)(2n-2)\cdots(6)(4)(2)] &= (2n)!\\
[(2n-1)(2n-3)\cdots(5)(3)(1)]\,[2^n(n)(n-1)\cdots(3)(2)(1)] &= (2n)!\\
[(2n-1)(2n-3)\cdots(5)(3)(1)]\,2^n n! &= (2n)!\\
(2n-1)(2n-3)\cdots 5\cdot 3\cdot 1 &= \frac{(2n)!}{2^n n!} \qquad (1)
\end{aligned}$$

Learning outcomes:

b. *It is easy to see that*

$$(n+1)(n+2)\cdots(2n) = \frac{(2n)!}{n!}$$

Using equation 1, we see that

$$\begin{aligned}\frac{(n+1)(n+2)\cdots(2n)}{2^n} &= \frac{(2n)!}{2^n n!}\\ &= (2n-1)(2n-3)\cdots 5\cdot 3\cdot 1 \in N\end{aligned}$$

so $n_0 = \prod_{k=1}^{n}(n+k)$ *is divisible by* 2^n*. Furthermore, the quotient of* $\frac{n_0}{2^n}$ *is odd, since the product of odd numbers is always odd. Thus,* $\frac{n_0}{2^n}$ *is not divisible by 2, and thus* n_0 *is not divisible by* 2^{n+1}*, because if it were,* $\frac{n_0}{2^{n+1}} = \frac{n_0/2^n}{2}$ *would be an integer, which we have shown is impossible.*

Problem 2 *Prove that if* p *is a prime and* $a^2 \equiv b^2 (mod\ p)$*, then* $p \mid (a+b)$ *or* $p \mid (a-b)$*.*

Solution.

Let p *be a prime number. If* $a^2 \equiv b^2 \mod p$ *then*

$$\begin{aligned}a^2 &\equiv b^2 \mod p\\ p &\mid a^2 - b^2\\ p &\mid (a+b)(a-b)\end{aligned}$$

By the following theorem (covered in class), p *must divide* $(a+b)$ *or* $(a-b)$*.*

Theorem 1. *Let* p *be a prime and* a*,* b *be integers. If* $p \mid ab$ *then* $p \mid a$ *or* $p \mid b$*.*

Problem 3 *Prove that* 19 *is not a divisor of* $4n^2 + 4$ *for any integer* n*.*

Solution.

We want to show that $19 \not| 4n^2 + 4$ *for any* $n \in \mathbb{Z}$*.*

In class, we showed that $x^2 \equiv -1 \mod p$ *for a given prime* p *if and only if* $p = 2$ *or* $p \equiv 1 \mod 4$*.*

Since $19 \equiv 3 \not\equiv 1 \mod 4$*, we see that for any* $n \in \mathbb{Z}$*,*

$$\begin{aligned}n^2 &\not\equiv -1 \mod 19\\ n^2 + 1 &\not\equiv 0 \mod 19\\ 4(n^2+1) &\not\equiv 0 \mod 19 \quad \textit{since } (4,19) = 1\\ 4n^2 + 4 &\not\equiv 0 \mod 19\\ 19 &\not| (4n^2 + 4).\end{aligned}$$

Problem 4 *Prove that $n^7 - n$ is divisible by 42, for any integer n.*

Solution.

We know by Fermat's Little Theorem that $n^1 - 1 \equiv 0 \pmod 2$, $n^2 - 1 \equiv 0 \pmod 3$ and $n^6 - 1 \equiv 0 \pmod 7$. We also know that $(n^i - 1) \mid (n^6 - 1)$ for $i = 1, 2, 6$. Hence, $n^7 - n \equiv 0 \pmod p$ for $p = 2, 3, 7$. Since $2, 3, 7$ are mutually relatively prime, we conclude that $n^7 - n \equiv 0 \pmod{2 \times 3 \times 7}$. Hence, $42 \mid (n^7 - n)$ for all integers n.

Problem 5 *Show that 2, 4, 6, . . . , 2m is the complete residue system for system modulo m if m is odd.*
Hint: Show that the set of remainders (mod m) of 2, 4, 6, . . . , 2m is 0, 1, 2, . . . , m-1.

Solution.

Suppose m is odd. Clearly, the set $\{1, 2, 3, \ldots, m\}$ is a complete residue system modulo m. Suppose $2 \cdot a \equiv 2 \cdot b \pmod m$. Since m is odd, $2 \not| m$, so $\gcd(2, m) = 1$. Hence, there exist c such that $2c \equiv 1 \pmod m$. Multiplying both sides of the equation, we get $(2c)a \equiv (2c)b \pmod m$ implying $a \equiv b \pmod m$. This is impossible if a, b are distinct elements of a complete residue system. So, $\{2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \ldots 2 \cdot m\} = \{2, 4, 6, \ldots 2m\}$ is also a complete residue system modulo m.

Problem 6 *For m odd, prove that the sum of the elements of any complete residue system modulo m is congruent to zero modulo m; prove the analogous result for any reduced residue system for $m > 2$.*

Solution.

Let m be odd. Clearly, $1, 2, 3, \ldots, m$ is a complete residue system. By definition, for any other complete residue system $r_1, r_2, r_3, \ldots, r_m$, each $r_i \equiv j_i$ for $1 \le i \le m$ and a unique $1 \le j_i \le m$. Thus, we may write the sum of elements as

$$\begin{aligned}
\sum_{i=1}^{m} r_i &= \sum_{i=1}^{m} (j_i + k_i m) && \text{where } j_i + k_i m = r_i, k_i \in \mathbb{Z} \\
&= \sum_{i=1}^{m} j_i + \sum_{i=1}^{m} k_i m \\
&= \sum_{j=1}^{m} j + \sum_{i=1}^{m} k_i m && \text{since each } j_i \text{ is unique} \\
&= \frac{m(m+1)}{2} + m \sum_{i=1}^{m} k_i \\
&= m \left(\frac{(m+1)}{2} + \sum_{i=1}^{m} k_i \right).
\end{aligned}$$

Clearly, $\sum_{i=1}^{m} k_i \in \mathbb{Z}$. Since m is odd, $\frac{m+1}{2} \in \mathbb{Z}$, so $\left(\frac{(m+1)}{2} + \sum_{i=1}^{m} k_i \right) \in \mathbb{Z}$ and

$$m \,\Big|\, \sum_{i=1}^{m} r_i$$

for any complete residue system $r_1, r_2, \ldots, r_m$ modulo m.

Now we aim to prove the analogous result for a reduced residue system given any $m > 2$. Let U_m represent the group of units modulo m whose elements are less than m. A unit is an element of $\mathbb{Z}_m$ which has an inverse under multiplication. We have shown that an element $a \in Z_m$ will have an inverse if $\gcd(a, m) = 1$. Clearly, U_m a reduced residue system.

First we aim to show that if $a \in U_m$, then $m - a \in U_m$. Assume $\gcd(a, m) = 1$. *We already know that* $\gcd(a, m) = \gcd(-a, m) = \gcd(-a + mx, m)$ *for any $x \in \mathbb{Z}$. Choose $x = 1$. Thus,*

$$1 = \gcd(a, m) = \gcd(m - a, m),$$

so $a \in U_m$ if and only if $m - a \in U_m$. (Note that the sum of these two numbers, a and $m - a$, is equal to m.)

Next we aim to show that there is no such element $a' \in \mathbb{Z}$ where $a' = m - a'$ and $\gcd(m, a') = 1$. *If $a' = m - a'$, then $a' = \frac{m}{2}$. If m is odd, no such number exists, so we assume that m is even. Thus, $\frac{m}{2} \in \mathbb{N}$. Clearly,*

$$\gcd(a', m) = \gcd\left(\frac{m}{2}, m\right) = \frac{m}{2}.$$

We see that $\frac{m}{2} = 1$ only when $m = 2$. For all other positive numbers, no such a' exists. Thus, for every $a \in U_m$, where $m > 2$, there will be a $b \in U_m$ such that $a \neq b$ and $a + b = m$. This also implies that $|U_m|$ is even for $m > 2$.

Going on we will show that the reduced residue system $r_1, r_2, \ldots, r_s$, for $s \in \mathbb{N}$ where $r_i < m$ for $1 \leq i \leq s$ the elements sum to a number divisible by m if $m > 2$. Suppose $m > 2$. For a given $r_i \in U_m$, we have shown that there will be another $r_j \in U_m$, where $i \neq j$ and $r_i + r_j = m$. Noting that $s = |U_m|$, we see that

$$\sum_{i=1}^{s} r_i = \frac{s}{2} m,$$

where $\frac{s}{2} \in \mathbb{N}$ because the cardinality of U_m is even. Therefore,

$$m \mid \sum_{i=1}^{s} r_i.$$

Finally, we show that the above result holds for any reduced residue system. Consider the reduced residue system $q_1, q_2, \ldots, q_{s'}$. Since each reduced residue system has the same number of elements ($\phi(m)$), $s' = s$. Each element q_i is congruent to a unique r_j modulo m for $1 \leq i, j \leq m$. Put another way, $q_i = r_j + km$ for some $k \in \mathbb{Z}$. Since the ordering of our set does not matter, we will say $q_i \equiv r_i \mod m$ for each $1 \leq i \leq m$. Now we have

$$\begin{aligned}
\sum_{i=1}^{s} q_i &= \sum_{i=1}^{s} (r_i + k_i m) && (k_i \in \mathbb{Z}) \\
&= \sum_{i=1}^{s} r_i + \sum_{i=1}^{s} k_i m \\
&= \frac{s}{2} m + m \sum_{i=1}^{s} k_i \\
&= m \left(\frac{s}{2} + \sum_{i=1}^{s} k_i \right).
\end{aligned}$$

Since $\frac{s}{2} \in \mathbb{Z}$ and $\sum_{i=1}^{s} k_i \in \mathbb{Z}$, $\left(\frac{s}{2} + \sum_{i=1}^{s} k_i \right) \in \mathbb{Z}$. By definition, $m \mid \sum_{i=1}^{s} q_i$. Since the choice of a reduced residue system $q_1, q_2, \ldots, q_s$ was arbitrary, the condition that m divides the sum of the elements of a reduced residue system modulo m holds if $m > 2$.

Problem 7 *Let p be a prime factor of $a^2 + 2b^2$. Show that if p does not divide both a and b, then the congruence $x^2 \equiv -2 (mod\ p)$ has a solution.*

Solution.

Let p be prime. Suppose $p \mid a^2 + 2b^2$ for $a, b \in \mathbb{Z}$. Since $p \nmid a, b$; $\gcd(p, a) = \gcd(p, b) = 1$. *Then, there exists $\bar{b} \in \mathbb{Z}_p$*

such that $\bar{b}b = b\bar{b} \equiv 1 \pmod{p}$. *We have*

$$\begin{aligned} p &\mid a^2 + 2b^2 \\ a^2 + 2b^2 &\equiv 0 \pmod{p} \\ a^2 &\equiv -2b^2 \pmod{p} \\ a^2\bar{b}^2 &\equiv -2b^2\bar{b}^2 \pmod{p} \\ \left(a\bar{b}\right)^2 &= -2\left(b\bar{b}\right)^2 \\ \left(a\bar{b}\right)^2 &\equiv -2 \pmod{p}. \end{aligned}$$

Thus, for $x = a\bar{b}$,

$$\begin{aligned} x^2 &= \left(a\bar{b}\right)^2 \\ &\equiv -2 \pmod{p}, \end{aligned}$$

so the congruence $x^2 \equiv -2 \mod p$ *has a solution if* $p \mid a^2 + 2b^2$ and $p \not| a, b$.

Problem 8 *How many solutions are there to the following congruences:*

(a) $15x \equiv 25 \mod 35$

(b) $15x \equiv 24 \mod 35$

(c) $15x \equiv 0 \mod 35$?

Solution.

We use our discussion on the existence of inverse modulo p *in class to determine the number of solutions.*

a. *A solution exists to the congruence*

$$\begin{aligned} 15x &\equiv 25 \pmod{3}5 \\ 3x &\equiv 5 \pmod{7} \\ 6x &\equiv 10 \pmod{7} \\ -1x &\equiv 3 \pmod{7} \\ x \equiv -3 &\equiv 4 \pmod{7} \end{aligned}$$

because $g = gcd(15, 35) = 5$, *and* $5 \mid 25$. *Furthermore, there are* $g = 5$ *solutions modulus 35:*

$$\{4, 4+7 = 11, 4+14 = 18, 4+21 = 25, 4+28 = 32\}$$

b. *No solution exists to the congruence*

$$15x \equiv 24 \mod 35$$

because $g = gcd(15, 35) = 5$, *and* $5 \not| 24$.

c. *A solution exists to the congruence*

$$15x \equiv 0 \mod 35$$

because $g = gcd(15, 35) = 5$, *and* $5 \mid 0$. *Furthermore, there are* $g = 5$ *solutions modulus 35.*

Problem 9 *Show that if p is an odd prime then the congruence $x^2 \equiv 1 \mod p^\alpha$ has only two solutions $x \equiv 1, x \equiv -1 \mod p^\alpha$.*

Solution.

Let p be an odd prime. We have

$$x^2 \equiv 1 \mod p^\alpha.$$

From this we see that

$$\begin{aligned} x^2 - 1 &\equiv 0 \mod p^\alpha \\ p^\alpha &\mid x^2 - 1 \\ p^\alpha &\mid (x+1)(x-1). \end{aligned} \tag{2}$$

This also implies

$$p \mid (x+1)(x-1).$$

As discussed previously, p divides at least one of the factors on the right.

Next we aim to show that p cannot divide both $x + 1$ and $x - 1$. If it did, then

$$\begin{aligned} &p \mid 1 \cdot (x+1) + (-1) \cdot (x-1) \\ &p \mid 2. \end{aligned}$$

$p \mid 2$ implies $p \leq 2$. Because 2 is the smallest prime number, $p \leq 2$ implies $p = 2$ since p is prime. But we assumed p is odd, which is a contradiction since 2 is even. Thus, p cannot divide one of these terms. Since the term that p divides doesn't matter, we'll say that p divides $x + 1$ but not $x - 1$.

We know that $\gcd(p, x-1) = 1$. Hence, $(x - 1)$ has not factor p^k for $k \geq 1$. So, $\gcd(p^\alpha, x-1) = 1$. Hence, in equation 2, we see that $p^\alpha \mid (x + 1)$. Since the term we assumed that p could divide was arbitrary, this analysis also works if p were to divide $x - 1$ but not $x + 1$.

Problem 10 *Find all integers that give remainders 1, 2, 3 when divided by 3, 4, 5, respectively.*

Solution.

We are being asked to solve the system of linear congruences

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 4 \\ x &\equiv 3 \mod 5. \end{aligned}$$

We start with the third congruence. The solution is $x = 3 + 5b$, for $b \in \mathbb{Z}$. Now we use this value in the second congruence to get

$$\begin{aligned} 3 + 5b &\equiv 2 \mod 4 \\ 5b &\equiv -1 \mod 4 \\ b &\equiv -1 \mod 4 \\ b &\equiv 3 \mod 4, \end{aligned}$$

so $b = 3 + 4c$, for $c \in \mathbb{Z}$. We plug this in to get

$$\begin{aligned} x &= 3 + 5b \\ &= 3 + 5(3 + 4c) \\ &= 3 + 15 + 20c \\ &= 18 + 20c \end{aligned}$$

Next, we use this for the first congruence

$$\begin{aligned} 18 + 20c &\equiv 1 \mod 3 \\ 2c &\equiv 1 \mod 3 \\ 2c &\equiv 4 \mod 3 \\ c &\equiv 2 \mod 3 && \textit{(because } \gcd(2,3) = 1 \end{aligned}$$

so $c = 2 + 3d$*, for* $d \in \mathbb{Z}$*.*

Finally, we have

$$\begin{aligned} x &= 18 + 20c \\ &= 18 + 20(2 + 3d) \\ &= 18 + 40 + 60d \\ &= 58 + 60d, \end{aligned}$$

which is the solution to all three congruences.

Problem 11 *Determine whether the congruences* $5x \equiv 1 \mod 6$ *and* $4x \equiv 13 \mod 15$ *have a common solution, and find them if they exist.*

Solution.

We aim to find whether or not the system of linear congruences

$$\begin{aligned} 5x &\equiv 1 \pmod 6 \\ 4x &\equiv 13 \pmod 1)5 \end{aligned}$$

has a solution, and if so what it is.

Using the congruence theorems covered in class, we see that

$$5x \equiv 1 \pmod 6$$

implies

$$\begin{aligned} 5x &\equiv 1 \pmod 3 \\ 2x &\equiv 4 \pmod 3 \\ 2(2x) = 4x \equiv x &\equiv 2(4) \equiv 2 \pmod 3, && \textit{(because } \gcd(2,3) = 1 \textit{ and } 2^2 \equiv 1 \pmod 3 \end{aligned} \tag{3}$$

and

$$4x \equiv 13 \pmod 1)5$$

implies

$$\begin{aligned} 4x &\equiv 13 \pmod 3 \\ 10(4x) &\equiv 10(13) \pmod 3 \\ x &\equiv 1 \mod 3. \end{aligned} \tag{4}$$

Clearly, equations 3 and 4 are incompatible because $1 \not\equiv 2 \mod 3$*. Thus, the system of linear congruences is inconsistent and no solutions exist.*

Problem 12 *Solve the congruence* $x^2 + 2x - 3 \equiv 0 \mod m$ *for* $m = 9, 5, 45$*.*

Solution.

We aim to solve the system of congruences

$$\begin{aligned} x^3 + 2x - 3 &= 0 \mod 9 \\ x^3 + 2x - 3 &= 0 \mod 5 \\ x^3 + 2x - 3 &= 0 \mod 45. \end{aligned}$$

It is worth noting that the first two congruences are implied by the third.

We solve for the first two congruences and use the Chinese remainder theorem to find solutions in $\mathbb{Z}_{45}$.

Plugging in $x = 0, 1, 2, \ldots, 8$, *we find that the soltions to the first congruence are* $x = 1, 2, 6 \mod 9$. *Likewise, by plugging in* $x = 0, 1, 2, 3, 4, 5$, *we find that the solutions to the second congruence are* $x = 1, 3 \mod 5$.

We see that $\gcd(5, 9) = 1$ *and* $45 = 5 \cdot 9$, *so the number of solutions* $N(45) = N(5)N(9) = 2 \cdot 3 = 6$ *for* $f(x) = x^3 + 2x - 3$. *All that needs to be done at this point is to use the Chinese remainder theorem to show six solutions in* $\mathbb{Z}_{45}$.

I will calculate the first solution for brevity. The algorithm for finding solutions is the same for the remaining five.

Let's find solutions to

$$\begin{aligned} x &\equiv 1 \mod 9 \\ x &\equiv 1 \mod 5 \end{aligned}$$

We start with $x = 1 + 9a$ *for* $a \in \mathbb{Z}$ *and plug it into the second congruence*

$$\begin{aligned} 1 + 9a &\equiv 1 \mod 5 \\ 9a &\equiv 0 \mod 5 \\ 9a &\equiv 90 \mod 5 \\ a &\equiv 10 \mod 5 && \text{(because } \gcd(9, 5) = 0\text{)} \\ a &\equiv 0 \mod 5, \end{aligned}$$

so $a = 0 + 5b$. *Plugging this into our first solution, we get*

$$\begin{aligned} x &= 1 + 9a \\ &= 1 + 9(0 + 5b) \\ &= 1 + 45b, \end{aligned}$$

so $x \equiv 1 \mod 45$.

Finding the remaining five solutions is similarly tedious. The six solutions are

$$\begin{aligned} x &\equiv 1 \mod 45 \\ x &\equiv 6 \mod 45 \\ x &\equiv 11 \mod 45 \\ x &\equiv 28 \mod 45 \\ x &\equiv 33 \mod 45 \\ x &\equiv 38 \mod 45 \end{aligned}$$

Problem 13 *Solve the congruence* $x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 503$.
Hint: 503 is prime and $x^3 - 9x^2 + 23x - 15 = (x - 1)(x - 3)(x - 5)$.

Solution.

We aim to solve the congruence

$$x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 503.$$

We are given 503 is prime and that

$$x^3 - 9x^2 + 23x - 15 = (x - 1)(x - 3)(x - 5).$$

We see that

$$\begin{aligned} x^3 - 9x^2 + 23x - 15 &\equiv 0 \mod 503 \\ 503 &\mid x^3 - 9x^2 + 23x - 15 \\ 503 &\mid (x-1)(x-3)(x-5). \end{aligned}$$

Since 503 is prime, at least one of these terms is divisible by 503.

From this we can find the following solutions

$$\begin{aligned} 503 &\mid (x-1) \\ x - 1 &\equiv 0 \mod 503 \\ x &\equiv 1 \mod 503 \end{aligned} \qquad \begin{aligned} 503 &\mid (x-3) \\ x - 3 &\equiv 0 \mod 503 \\ x &\equiv 3 \mod 503 \end{aligned} \qquad \begin{aligned} 503 &\mid (x-5) \\ x - 5 &\equiv 0 \mod 503 \\ x &\equiv 5 \mod 503 \end{aligned}$$