Homework 2 – Number Theory and Counting

Exercise 1. Calculate the greatest common divisors of numbers shown below and express this value in the form of the Bézout identity.

(a) $\gcd(12, 17)$ (b) $\gcd(27, 12)$ (c) $\gcd(65, 5)$ (d) $\gcd(10, 27)$

Solution.

(a) $\gcd(12, 17) = (-7) \cdot 12 + 5 \cdot 17 = 1$

(b) $\gcd(27, 12) = 1 \cdot 27 + (-2) \cdot 12 = 3$

(c) $\gcd(65, 5) = 0 \cdot 65 + 1 \cdot 5 = 5$

(d) $\gcd(10, 27) = (-8) \cdot 10 + 3 \cdot 27 = 1$

Exercise 2. Answer the questions below.

(a) Which integers are congruent to 3 mod 7?

(b) List integers in the equivalence class of 5 mod 10?

Solution.

(a) Integers congruent to 3 mod 7 are:

$$[3] = \{\ldots, -18, -11, -4, 3, 10, 17, 24, \ldots\} \ .$$

(b) The equivalence class of 5 mod 10 is

$$[5] = \{\ldots, -35, -25, -15, -5, 5, 15, 25, 35, \ldots\} \ .$$

Exercise 3. Calculate

(a) 3 mod 5	(b) 5 mod 3	(c) 12 mod 3	(d) 7 mod 4
(e) -5 mod 8	(f) -4 mod 11	(g) 6^{-1} mod 7	(h) 2^{-1} mod 6

Solution.

(a) 3	(b) 2	(c) 0	(d) 3
(e) 3	(f) 7	(g) 6	(h) none exists

In (g), one can see that $6^{-1} = 6 \pmod 7$, since $6 \cdot 6 = 36 \equiv 1 \pmod 7$. In (h), one can see that 2 is not invertible modulo 6, since $\gcd(2, 6) = 2 \neq 1$.

Exercise 4. Solve for x. If the equation is not solvable, provide a justification for it.

(a) $x + 12 \equiv 7 \pmod{15}$ (b) $4x \equiv 3 \pmod 7$

(c) $15x + 12 \equiv 21 \pmod{27}$ (d) $8x \equiv 3 \pmod{28}$

Solution.

(a) Subtracting 12 from both sides of the equation we obtain the solution $x \equiv 10 \pmod{15}$

(b) Multiplying both sides of the equation by 2, we obtain the solution $x \equiv 6 \pmod{7}$

(c) Subtracting 12 from both sides of the equation we get $15x \equiv 9 \pmod{27}$. Since $\gcd(15, 27) = 3$ and $3|9$, then by dividing all three parameters of the equation by 3, we obtain the reduced form $5x \equiv 3 \pmod{9}$. Multiplying both sides of this equation by 2, we get the solution $x \equiv 6 \pmod{9}$. To verify, observe that $15 \cdot 6 + 12 = 102 \equiv 21 \pmod{27}$.

(d) Since $\gcd(8, 28) = 4$, but $3 \nmid 4$, this equation is not solvable.

Exercise 5. Solve for x. If the system is not solvable, provide a justification for it.

$$(a) \quad \begin{cases} 5a + b \equiv 0 \pmod{8} \\ 2a + b \equiv 1 \pmod{8} \end{cases} \qquad (b) \quad \begin{cases} 3a + b \equiv 6 \pmod{7} \\ 6a + b \equiv 4 \pmod{7} \end{cases}$$

$$(c) \quad \begin{cases} 5a + b \equiv 4 \pmod{6} \\ 3a + b \equiv 5 \pmod{6} \end{cases} \qquad (d) \quad \begin{cases} 9a + b \equiv 1 \pmod{10} \\ 5a + b \equiv 5 \pmod{10} \end{cases}$$

Solution.

(a) Subtracting the second equation from the first one, we get $3a \equiv 7 \pmod{8}$. Multiplying both sides of the equation by 3, we get $a \equiv 5 \pmod{8}$. From the first equation, we see that $b = -5a = -25 \equiv 7 \pmod{8}$. Hence, $a \equiv 5 \pmod{8}, b \equiv 7 \pmod{8}$.

(b) Subtracting the first equation from the second, we get $3a \equiv 5 \pmod{7}$. Multiplying both sides of the equation by 5, we get $a \equiv 4 \pmod{7}$. From the first equation, we get $b = 6-3a = -6 \equiv 1 \pmod{7}$. Hence, $a \equiv 4 \pmod{7}, b \equiv 1 \pmod{7}$.

(c) Subtracting the second equation from the first one, we get $2a \equiv 5 \pmod{6}$. Since $\gcd(2, 6) = 2$ and $2 \nmid 5$, the system has no solutions.

(d) Subtracting the second equation from the first one, we get $4a \equiv 6 \pmod{10}$. Since $\gcd(4, 10) = 2$ and $2|6$, by dividing the equation by 2, we get $2a \equiv 3 \pmod{5}$. Multiplying both sides of the equation by 3, we get $a \equiv 4 \pmod{5}$. From the first equation, we have $b = 1 - 9a = -35 \equiv 5 \pmod{10}$. Hence, $a \equiv 4 \pmod{10}, b \equiv 5 \pmod{10}$.

Exercise 6. Solve for x.

$$(a) \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases} \qquad (b) \quad \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 7 \pmod{9} \end{cases}$$

$$(c) \quad \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \\ x \equiv 6 \pmod{8} \end{cases} \qquad (d) \quad \begin{cases} x \equiv 6 \pmod{10} \\ x \equiv 3 \pmod{13} \\ x \equiv 15 \pmod{19} \end{cases}$$

Solution.

(*a*) By the Bézout identity, $\gcd(3,5) = 2\cdot 3 + (-1)\cdot 5 = 1$. Therefore, $x \equiv 4\cdot 3\cdot 2 + 2\cdot(-1)\cdot 5 \equiv 14 \pmod{15}$.

(*b*) By the Bézout identity, $\gcd(4,9) = (-2)\cdot 4 + 1\cdot 9 = 1$, and therefore $x \equiv 7\cdot 4\cdot(-2) + 3\cdot 1\cdot 9 = -29 \equiv 7 \pmod{36}$.

(*c*) $N = 5\cdot 7\cdot 8 = 280$, $N_1 = \frac{280}{5} = 56$, $N_2 = \frac{280}{7} = 40$, $N_3 = \frac{280}{8} = 35$, $\gcd(56,5) = 1\cdot 56 - 11\cdot 5 = 1$, $\gcd(40,7) = 3\cdot 40 - 17\cdot 7 = 1$, $\gcd(35,8) = 3\cdot 35 - 13\cdot 8 = 1$, $x \equiv 3\cdot 1\cdot 56 + 5\cdot 3\cdot 40 + 6\cdot 3\cdot 35 = 1398 \equiv 278 \pmod{280}$.

(*d*) $N = 10\cdot 13\cdot 19 = 2470$, $N_1 = \frac{2470}{10} = 247$, $N_2 = \frac{2470}{13} = 190$, $N_3 = \frac{2470}{19} = 130$, $\gcd(247,10) = 3\cdot 247 - 74\cdot 10 = 1$, $\gcd(190,13) = 5\cdot 190 - 73\cdot 13 = 1$, $\gcd(130,19) = 6\cdot 130 - 41\cdot 19 = 1$, $x \equiv 6\cdot 3\cdot 247 + 3\cdot 5\cdot 190 + 15\cdot 6\cdot 130 = 18996 \equiv 1706 \pmod{2470}$.

Exercise 7. Calculate the value of the Euler's totient function $\varphi(n)$.

(*a*) $\varphi(11)$	(*b*) $\varphi(99)$
(*c*) $\varphi(20)$	(*d*) $\varphi(540)$

Solution.

(*a*) Since 11 is a prime number, $\varphi(11) = 10$.

(*b*) The prime factorization of 99 is $99 = 3^2\cdot 11$, hence $\varphi(99) = 99\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{11}\right) = 60$.

(*c*) The prime factorization of 20 is $20 = 2^2\cdot 5$, hence $\varphi(20) = 20\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right) = 8$.

(*d*) $540 = 2^2\cdot 3^3\cdot 5$, hence $\varphi(540) = 540\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right) = 144$.

Exercise 8. (Reimo Palm) Andy has 5 toy ships and 6 toy planes. He wants to make an exhibition showing 3 models of one kind and 4 models of the other kind. How many ways there are to pick the exhibition set from his collection?

Solution. The exhibition may consist of either 3 ships and 4 planes or 4 ships and 3 planes, and thus there are $\binom{5}{3}\cdot\binom{6}{4} + \binom{5}{4}\cdot\binom{6}{3} = 10\cdot 15 + 5\cdot 20 = 250$ possible sets.

Exercise 9. How many ways there are to line up n male and $n-1$ female students for a group photo so that in the resulting arrangement no two males stand side by side?

Solution. To avoid placing two males next to each other, the only option is to alternate males and females, starting from a male. There are $n!$ ways to arrange the n males among the n odd-numbered positions, and $(n-1)!$ ways to arrange the $n-1$ females among the $n-1$ even-numbered positions in the line. Any arrangement of males can be combined with any arrangement of females, so we have $n!(n-1)!$ possibilities in total.

Exercise 10. Solve the recurrence $A_{n+2} = A_{n+1} + 2A_n + 1$, when $A_0 = 0$, $A_1 = 2$.

Solution. We can obtain the solution with the 3-step method shown in the lecture:

- The corresponding homogeneus recurrence is $A'_{n+2} = A'_{n+1} + 2A'_n$. Its characteristic equation $q^2 - q - 2 = 0$ gives $q_1 = 2$, $q_2 = -1$. Thus the general solution is $A'_n = c_1 2^n + c_2(-1)^n$.

- Generalizing the non-homogeneus member, we will look for particular solutions of the form $A''_n = \alpha \cdot n + \beta$. Substituting into the recurrent rule, we get $(\alpha \cdot (n+2) + \beta) = (\alpha \cdot (n+1) + \beta) + 2(\alpha \cdot n + \beta) + 1$. Collecting like terms, we get $2\alpha \cdot n + 2\beta - \alpha + 1 = 0$. Since this has to hold for all n, we have $2\alpha = 0$, or $\alpha = 0$, and $2\beta - \alpha + 1 = 0$, or $\beta = -\frac{1}{2}$. Thus $A''_n = 0 \cdot n - \frac{1}{2} = -\frac{1}{2}$.
- The solution for the original recurrence must then be of the form $A_n = c_1 2^n + c_2(-1)^n - \frac{1}{2}$. Looking at the boundary conditions, we have $A_0 = c_1 + c_2 - \frac{1}{2} = 0$ and $A_1 = 2c_1 - c_2 - \frac{1}{2} = 2$ giving $c_1 = 1$, $c_2 = -\frac{1}{2}$, for the solution

$$A_n = 1 \cdot 2^n + (-\frac{1}{2}) \cdot (-1)^n - \frac{1}{2} = 2^n - \frac{(-1)^n + 1}{2}.$$

Alternatively, we could compute a few more elements ($A_2 = A_1 + 2A_0 + 1 = 2 + 2 \cdot 0 + 1 = 3$, $A_3 = A_2 + 2A_1 + 1 = 8$, $A_4 = 15$, $A_5 = 32$, $\ldots$), postulate the hypothesis

$$A_n = \begin{cases} 2^n & \text{if } n \text{ is odd,} \\ 2^n - 1 & \text{if } n \text{ is even,} \end{cases}$$

and then prove it by induction (which will be covered later in the course).

For the base case, we can immediately verify $2^0 - 1 = 1 - 1 = 0 = A_0$, $2^1 = 2 = A_2$. For the induction step, let's first consider A_{n+2} for even n. Then $n+1$ is odd and $n+2$ is even, and we have $A_{n+2} = A_{n+1} + 2A_n + 1 = 2^{n+1} + 2(2^n - 1) + 1 = 2^{n+1} + 2 \cdot 2^n - 2 + 1 = 2^{n+2} - 1$, as it should be for even $n+2$. Considering A_{n+2} for odd n, we get similarly $A_{n+2} = 2^{n+1} - 1 + 2 \cdot 2^n + 1 = 2^{n+2}$, which completes the proof that the hypothesis holds for all $n \geq 0$.

Finally, note that the two formulae are really the same, as the term $\frac{(-1)^n+1}{2}$ is 0 when n is odd and 1 when n is even.