MATH 381 HW 9 part 3

Christian Jahnel

27 March 2024

1. Find gcd(620, 140).

$$\begin{aligned} 620 &= 4(140) + 60 \iff 60 = 620 - 4(140) \\ 140 &= 2(60) + 20 \iff 20 = 140 - 2(60) \\ 60 &= 3(20) + 0 \end{aligned}$$

   $\therefore \gcd(620, 140) = 20$

2. Show that an integer $a \in \mathbb{Z}_n$ has a multiplicative inverse, that is, an element $a^{-1} \in \mathbb{Z}_n$ with $a \cdot_n (a^{-1}) = 1$, if and only if a and n are relatively prime.

   Assume $(a, n) = 1$. By Bézout's Theorem, $\exists s, t \in \mathbb{Z}$ such that

$$\begin{aligned} a \cdot s + n \cdot t &= 1 \\ a \cdot s + n \cdot t &\equiv 1 \pmod{n} \\ n \cdot t &\equiv 0 \pmod{n} \\ \implies a \cdot s &\equiv 1 \pmod{n} \\ \implies a^{-1} &= \hat{s} \in \mathbb{Z}_n \end{aligned}$$

   Now assume a has a multiplicative inverse, i.e. $\exists \hat{x} \in \mathbb{Z}_n$ such that

$$\begin{aligned} \hat{a} \cdot \hat{x} &= \hat{1} \qquad \mathbb{Z}_n \\ \implies n &\mid ax - 1 \\ \implies \exists y \in \mathbb{Z} \quad ny &= ax - 1 \\ \iff ax - ny &= 1 \end{aligned}$$

$$\text{Assume } \begin{cases} d \mid a \\ d \mid n \end{cases} \implies d \mid ax - ny \implies d \mid 1$$
$$\therefore d = 1 \implies (a, n) = 1 \quad \blacksquare$$

3. The numbers 307 and 220 are relatively prime.

   (a) Find integers x and y satisfying $307x + 220y = 1$.

$$\begin{aligned} 307 &= 220 + 87 \iff 87 = 307 - 220 \\ 220 &= 2(87) + 46 \iff 46 = 220 - 2(87) \\ 87 &= 46 + 41 \iff 41 = 87 - 46 \\ 46 &= 41 + 5 \iff 5 = 46 - 41 \\ 41 &= 8(5) + 1 \iff 1 = 41 - 8(5) \\ 5 &= 5(1) + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 41 - 8(5) \\ &= 41 - 8(46 - 41) \\ &= (87 - 46) - 8(46 - (87 - 46)) \\ &= (307 - 220 - (220 - 2(307 - 220))) - 8(220 - 2(307 - 220) \\ &\quad - (307 - 220 - (220 - 2(307 - 220)))) \end{aligned}$$
$$a = 307, b = 220$$
$$\begin{aligned} 1 &= (a - b - (b - 2(a - b))) - 8(b - 2(a - b) - (a - b - (b - 2(a - b)))) \\ &= (a - b - b + 2a - 2b) - 8(b - 2a + 2b - a + b + b - 2a + 2b) \\ &= 3a - 4b - 8(7b - 5a) \\ &= 3a - 4b - 56b + 40a \\ &= 43a - 60b = 307(43) + 220(60) = 1 \end{aligned}$$
$$\therefore x = 43, b = -60$$

   (b) Use the equation found in (a) to determine the multiplicative inverse of 307 in $\mathbb{Z}_{220}$.

$$\begin{aligned} 307x + 220y = 1 &\implies 307x + 220y \equiv 1 \pmod{220} \\ 220y \equiv 0 \pmod{220} &\implies 307x \equiv 1 \pmod{220} \\ &\implies x = 43 \equiv 307^{-1} \pmod{220} \end{aligned}$$

4. A U.S. Social Security number consists of 9 digits; the first digit may be a 0.

   (a) How many different Social Security numbers are there?

   $$10^9 = 1,000,000,000$$

   (b) How many Social Security numbers have all even digits?

   $$5^9 = 1,953,125$$

5. A group of 12 women and 12 men are to be lined up.

   (a) How many lines are there beginning with a woman and ending with a man?

   The line would look like this:
   W _ M
   Since we have 12 options for the woman at the beginning and 12 options for the man at the end, by the product rule these numbers multiply with the number of permutations of the remaining 22 people i.e. 22!.

   $$12 \cdot 22! \cdot 12 \approx 1.61856105 \times 10^{23}$$

   (b) How many lines are available if no two men are allowed to be adjacent?

   Since no two men are allowed to be adjacent, the line must alternate between a man and a woman. Therefore, we can reduce the problem to two situations depending on the gender of the first in line.

   i. MWMWMWMWMWMWMWMWMWMWMWMWMW
   ii. WMWMWMWMWMWMWMWMWMWMWMWMWM

   If we then only think about the order of the women and men separately, we can reduce the problem to the number of arrangements of men multiplied by the number of arrangements of women (by the product rule). We also have to multiply this by two since we consider two possibilities based on the gender of the person first in line.

$$
\begin{aligned}
P_M &= 12! \\
P_W &= 12! \\
P &= 2 \cdot (12! \cdot 12!) \\
&\approx 4.58885066 \times 10^{17}
\end{aligned}
$$

6. How many functions are there from $\mathbb{Z}_5$ to $\mathbb{Z}_n$, $n \geq 2$ that

   (a) are one-to-one?

$$
\begin{cases} n(n-1)(n-2)(n-3)(n-4) & n \geq 5 \\ 0 & n < 5 \end{cases}
$$

   (b) have 0 in the range?

   i. Only 1 element in Z_5 maps to 0
   5 options for the 0; other 4 in domain give n^4 options

   ii. 2 elements in Z_5 maps to 0
   $5 \cdot 4$ options for the 0s; other 3 in domain give n^3 options

   iii. 3 elements in Z_5 maps to 0
   $5 \cdot 4$ options for the nonzeros which give n^2 options

   iv. 4 elements in Z_5 maps to 0
   5 options for the non-zero which has n options

   v. All 5 elements in Z_5 maps to 0
   1 function which maps all to 0

$$
\begin{aligned}
&5n^4 + (5 \cdot 4)n^3 + (5 \cdot 4)n^2 + 5n + 1 \\
&= 5n^4 + 20n^3 + 20n^2 + 5n + 1
\end{aligned}
$$