MATH221 Mathematics for Computer Science

Outline Solutions to Tutorial Sheet Week 6

Autumn 2017

1. There are three types of pennies. If we pick 12 pennies, then we may have 4 pennies from each year. So 12 is not enough. If we pick 13 pennies (pigeons) and split them up according to their years (pigeonholes), then because $13 > 3 \times 4$, the generalised pigeonhole principle implies that we must have at least 5 pennies from the same year.

2.

(i) There are 15 possible remainders: $0, 1, 2, \ldots, 14$. So we need to choose 16 numbers. Then there are 15 possible remainders (pigeonholes) filled with 16 numbers (pigeons), and so by the pigeonhole principle two of the numbers must have the same remainder.

(ii) Notice that 9 numbers is not enough: the numbers $111, 222, \ldots, 999$ have nothing in common. So we need to choose 10 numbers. Then there are 9 possibilities for the first digit (pigeonholes) filled with our 10 choices (pigeons), and so by the pigeonhole principle two of the numbers must have the same first digit.

3. The $\gcd$ and the m, n follow from the repeated application of the quotient-remainder theorem:

$$\begin{aligned}
98 = 85 \times 1 + 13 &\implies 13 = 98 - 85 \times 1, & (1)\\
85 = 13 \times 6 + 7 &\implies 7 = 85 - 13 \times 6, & (2)\\
13 = 7 \times 1 + 6 &\implies 6 = 13 - 7 \times 1, & (3)\\
7 = 6 \times 1 + 1 &\implies 1 = 7 - 6 \times 1. & (4)
\end{aligned}$$

From here (we can omit the next equation, which would read $6 = 1 \times 6 + 0$) we know that $\gcd(98, 85) = 1$. Now we work backwards, starting from equation (4), and substituting for the remainder:

$$\begin{aligned}
1 &= 7 - 6 \times 1 && \text{(equation (4))}\\
&= 7 - (13 - 7 \times 1) \times 1 && \text{(using equation (3))}\\
&= 7 \times 2 - 13 \times 1 && \text{(simplifying)}\\
&= (85 - 13 \times 6) \times 2 - 13 \times 1 && \text{(using equation (2))}\\
&= 85 \times 2 - 13 \times 13 && \text{(simplifying)}\\
&= 85 \times 2 - (98 - 85 \times 1) \times 13 && \text{(using equation (1))}\\
&= 98 \times (-13) + 85 \times 15. && \text{(simplifying)}
\end{aligned}$$

Therefore, if we put $m = -13$ and $n = 15$, then we have $\gcd(98, 85) = 1 = 98m + 85n$.

For (ii) we work as in the previous question to find $\gcd(224, 1715) = 7$ and $7 = 224m + 1715n$, where $m = 23$ and $n = -3$.

4. Let $d = \gcd(a, b)$. If there is a prime p such that $p \mid a$ and $p \mid b$, then by the definition of the gcd we also have $p \mid d$, so $d \neq 1$. So, taking the contrapositive, if $d = 1$, then no such p exists.

If $d > 1$, then we know there is a prime p such that $p \mid d$. Since $d \mid a$ and $d \mid b$, we have $p \mid a$ and $p \mid b$ by the transitivity of divisibility.

5. The easy solution is to pick pairs of distinct prime numbers (11 and 13, for example), since their only common factor is 1. But the question asks us to make sure that some of the numbers involved are *not* primes, and lots of other choices are possible; Question 2 shows, for example, that $22 = 2 \times 11$ and $35 = 5 \times 7$ will do.

6. We have $-17 \equiv 7,\ 3 \equiv 3,\ 43 \equiv 7,\ 15 \equiv 3,\ 37 \equiv 1,\ -11 \equiv 1,\ -21 \equiv 3,$ all modulo 12.

7. We have

$$\begin{aligned} 6 \equiv m(\text{mod } 3) &\iff 3|(6-m) \\ &\iff 6-m = 3k \text{ for some } k \in \mathbb{Z} \\ &\iff m = 6-3k \text{ for some } k \in \mathbb{Z} \\ &\iff m \in \{\ldots,-3,0,3,6,9,12,\ldots\} \end{aligned}$$

Similarly, $m \equiv 125 \pmod 7$ if and only if $m = 125 - 7k$ for some $k \in \mathbb{Z}$. So the set of solutions is $\{\ldots,111,118,125,132,139,\ldots\}$.

8. We have

$$2^4 = 16 \equiv 1 \pmod 5.$$

So $2^{100} = (2^4)^{25} \equiv 1 \pmod 5$.

Using repeated squaring, and reducing modulo 7 whenever necessary, we find

$$\begin{array}{ccccccc} 3^1 & \equiv & 3 & & & & \\ 3^2 & = & 9 & \equiv & 2 & & \\ 3^4 & \equiv & 2^2 & = & 4 & & \\ 3^8 & \equiv & 4^2 & = & 16 & \equiv & 2 \\ 3^{16} & \equiv & 2^2 & = & 4 & & \\ 3^{32} & \equiv & 4^2 & = & 16 & \equiv & 2 \\ 3^{64} & \equiv & 2^2 & = & 4, & & \end{array}$$

where all congruences are modulo 7. Now, since $100 = 64 + 32 + 4$, we have

$$3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4 \equiv 4 \cdot 2 \cdot 4 \equiv 4 \pmod 7.$$

For the record, $3^{100} = 515377520732011331036461129765621272702107522001$.

9. Let $a, b \in \mathbb{Z}$. To prove that $[a] = [b] \iff a \equiv b \pmod n$, there are two things to prove: that $[a] = [b] \implies a \equiv b \pmod n$, and that $a \equiv b \pmod n \implies [a] = [b]$.

(i) We assume that $[a] = [b]$ and prove that $a \equiv b \pmod n$.
Let $x \in [a]$. Then $x \equiv a \pmod n$, by definition of $[a]$. Since $[a] = [b]$, we have $x \in [b]$ also. Hence $x \equiv b \pmod n$. Now, $x \equiv a \pmod n$ implies $a \equiv x \pmod n$, by the symmetry property of congruence. Now $x \equiv b \pmod n$, with the transitivity property, implies that $a \equiv b \pmod n$, as required.

(ii) We assume that $a \equiv b \pmod n$ and prove that $[a] = [b]$. To show that $[a] = [b]$, there are two things to prove: that $[a] \subseteq [b]$, and that $[b] \subseteq [a]$.
We assume that $a \equiv b \pmod n$ and prove that $[a] \subseteq [b]$. If $x \in [a]$, then $x \equiv a \pmod n$, by definition of congruence classes. Hence $x \equiv b \pmod n$ by transitivity, and so $x \in [b]$. Therefore, $[a] \subseteq [b]$.
The proof that if $a \equiv b \pmod n$ then $[b] \subseteq [a]$ is similar.

10. Here are the tables for $\mathbb{Z}_5$:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

×	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

11. (i) $[m] \in \mathbb{Z}_7$ is a set of numbers; $\mathbb{Z}_7$ is a set of sets.

(ii) $[2] = \{\dots, -26, -19, -12, -5, 2, 9, 16, 23, \dots\}$
$[5] = \{\dots, -23, -16, -9, -2, 5, 12, 19, 26, \dots\}$
$[7] = [0] = \{\dots, -28, -21, -14, -7, 0, 7, 14, 21, 28, \dots\}$
$\mathbb{Z}_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$.

(iii) (a) $[2] = [9]$ is true, since $2 \equiv 9 \pmod 7$.

(b) We could either say that $[5] = 5 \pmod 7$ is false since $[5]$ is a set while 5 is a number, or that it is meaningless since we have not introduced notation of the form "$\cdots = \cdots \pmod{\cdots}$".

(c) $5 \in [19]$ is true, since $5 \equiv 19 \pmod 7$.

(d) $3 \in \mathbb{Z}_7$ is false, since $\mathbb{Z}_7$ is a set of sets while 3 is a number.

(e) $[10] \in \mathbb{Z}_7$ is true, since $\mathbb{Z}_7$ is the set of *all* congruence classes modulo 7; of course, we usually prefer to write $[3]$ in place of $[10]$.

(f) $[a] \in [b]$ whenever $a \equiv b \pmod 7$ is false, since $[a]$ and $[b]$ are both sets of numbers, so $[a]$ cannot be in $[b]$.