MACM 101 — Discrete Mathematics I

Outline Solutions to Exercises on Integers

1. **Find the binary (base 2), octal (base 8), and hexadecimal (base 16) expasion of 1234567.**

   $(1234567)_2 = 100101101011010000111$

   $(1234567)_8 = 4553207$

   $(1234567)_{16} = 12D687$

2. **Add the hexadecimal numbers $49F7 + C66$.**

   Method 1. Convert the numbers into base 10, add them, and convert back.

   $$\begin{aligned} 49F7 &= 4 \cdot 16^3 + 9 \cdot 16^2 + 15 \cdot 16 + 7 = 18935, \\ C66 &= 12 \cdot 16^2 + 6 \cdot 16 + 6 = 3174. \end{aligned}$$

   Thus

   $$(49F7 + C66)_{16} = (18935 + 3174)_{10} = (22109)_{10} = (565D)_{16}.$$

   Method 2. Use the high-school algorithm only base 16:

   $$\begin{array}{cccc} & 4 & 9 & F & 7 \\ + & & & & \\ & & C & 6 & 6 \\ \hline & 5 & 6 & 5 & D \end{array}$$

3. **Find the greatest common divisor, the least common multiple of $a = 2475$ and $b = 32670$. Find numbers u, v such that $gcd(a, b) = ua + vb$.**

   We have $32670 = 13 \cdot 2475 + 495$ and then $2475 = 5 \cdot 495$. Thus $gcd(32670, 2475) = 495$. From the first equality we have $495 = 1 \cdot 32670 - 13 \cdot 2475$, and we can set $u = -13, v = 1$. Finally we have

   $$lcm(32670, 2475) = \frac{32670 \cdot 2475}{gcd(32670, 2475)} = 163,350.$$

4. **Prove that for any positive integers a, b it holds that $gcd(a, b) = gcd(a, a + b)$.**

   We prove that the pairs a, b and $a, a+b$ have the same common divisors. If $d \mid a, d \mid b$ then $d \mid a+b$ by Property (i) (see Slide 20-4). Conversely, if $d \mid a$ and $d \mid a + b$ then $d \mid b = (a + b) - a$ by property from Slide 20-5.

5. **Is it true that for any odd n the number $2^n + 1$ is divisible by 3? Prove your answer.**

   It is true, we prove it by induction. For $n = 1$ we have $2^1 + 1 = 3$, which is divisible by 3. Suppose that $2^k + 1$ is divisible by 3 and k is odd. Consider $2^{k+2} + 1$ (remember we should keep the exponent odd). We have

   $$2^{k+2} + 1 = 4(2^k + 1 - 1) + 1 = 4(2^k + 1) - 3,$$

   which is divisible by 3 as $2^k + 1$ and 3 are divisible by 3.

6. **Prove that there are no 3 consecutive odd prime numbers, that is, for any odd p, at least one of $p, p+2, p+4$ is composite.**

   Note: as stated the fact is false, since $p = 3, p + 2 = 5, p + 4 = 7$ is a sequence of 3 prime numbers. It is true for all $p \geq 5$. An equivalent statement, as shown in the proof below, which holds for all odd $p \geq 3$ is that every sequence of 3 consecutive odd numbers contains one number which is divisible by 3.

   Consider the result of dividing p by 3 — that is, $p = 3q + r$ where $0 \leq r \leq 2$. If $r = 0$ then p is divisible by 3. If $r = 1$, then $p + 2 = 3q + 3$ which is divisible by 3, and if $r = 2$ then $p + 4 = 3q + 6$ which is divisible by 3.

7. **Show that if a, b, and n are integers such that $n \geq 2$ and $a \equiv b \pmod{n}$, then $gcd(a, n) = gcd(b, n)$.**

   We have $a = b + n \cdot k$ for some integer k. By Lemma from slide 26-8 $gcd(a, n) = gcd(b, n)$ (in the notation of the Lemma a is a, n is b and b is r).

8. **Let m, n be positive integers, and let $f : \mathbb{Z}_m \to \mathbb{Z}_m$ be the function defined by $f(x) = nx \pmod{m}$. Prove that f is one-to-one if and only if $gcd(m, n) = 1$.**

   Suppose first $gcd(m, n) = d > 1$, then $m = kd, n = ld$ for some $k, l \in \mathbb{Z}$. Then

   $$f(k) = nk = kld = ml \equiv 0 \pmod{m}, \qquad f(2k) = 2nk = 2kld = 2ml \equiv 0 \pmod{m}.$$

   On the other hand, if $gcd(m, n) = 1$ then n has an inverse modulo m. Therefore if $f(a) = f(b)$ we have

   $$\begin{aligned} na &\equiv nb \pmod{m} \\ n^{-1}na &\equiv n^{-1}nb \pmod{m} \\ a &\equiv b \pmod{m} \end{aligned}$$

9. **Find the inverse of 11 modulo 47.**

   Apply Euclidean algorithm:

   $$\begin{aligned} 47 &= 4 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

   Therefore 11 has an inverse modulo 47, and we use the computation above to find it.

   $$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (11 - 3 \cdot 3) = 4 \cdot 3 - 1 \cdot 11 = 4(47 - 4 \cdot 11) - 1 \cdot 11 = 4 \cdot 47 - 17 \cdot 11.$$

   Thus $-17 \cdot 11 \equiv 30 \cdot 11 \equiv 1 \pmod{47}$, and 30 is the inverse of 11 modulo 47.

10. **Solve the congruence $3x \equiv 7 \pmod{19}$.**

    We have

    $$\begin{aligned} 3x &\equiv 7 \pmod{19} \\ 3^{-1}3x &\equiv 3^{-1}7 \pmod{19} \\ x &\equiv 13 \cdot 7 \pmod{19} \\ x &\equiv 15 \pmod{19} \end{aligned}$$