HAEF IB – FURTHER MATH HL
TEST IN NUMBER THEORY
by Christos Nikolaidis

SOLUTIONS
26-IV-2017

1. *[Maximum mark: 6]*

Let a and b be two positive integers. Show that $\gcd(a,b) \times \text{lcm}(a,b) = ab$

Solution

Let $p_1, ..., p_n$ be the set of primes that divide either a or b	M1
Then $a = p_1^{\alpha_2} p_2^{\alpha_2} ... p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} ... p_n^{\beta_n}$	A1A1
Hence $ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} ... p_n^{\alpha_n+\beta_n}$	A1
Furthermore $\min\{\alpha_j, \beta_j\} + \max\{\alpha_j, \beta_j\} = \alpha_j + \beta_j$ for $j = 1,2,...,n$	A1
Hence $ab = p_1^{\min\{\alpha_1,\beta_1\}+\max\{\alpha_1,\beta_1\}} ... p_n^{\min\{\alpha_n,\beta_n\}+\max\{\alpha_n,\beta_n\}}$	A1
$ab = \gcd(a,b) \times \text{lcm}(a,b)$	AG

2. *[Maximum mark: 12]*

(a) Show that if 3 divides $(a^2 + b^2)$ then 3 divides a and 3 divides b, where $a, b \in \mathbb{Z}^+$. *[5 marks]*

(b) Show that if p is a prime number and p divides a and p divides $(a^2 + b^2)$ then p divides b, where $a, b, p \in \mathbb{Z}^+$. *[3 marks]*

(c) The greatest common divisor of x and y is denoted by (x, y). Show that if a and b are relatively prime, then $(a, bc) = (a, c)$, where $a, b, c \in \mathbb{Z}^+$. *[4 marks]*

Solution

(a) Either $3|a$ or $3 \nmid a$ (for either a or b). ***(M1)***

In the second case either $a \equiv 1 \bmod 3$ or $a \equiv 2 \bmod 3$ (and the same for b), and in both cases it follows that $a^2 \equiv 1 \bmod 3$ and $b^2 \equiv 1 \bmod 3$, hence $a^2 + b^2 \equiv 1 \bmod 3$ (when one of them is divisible by 3) or $a^2 + b^2 \equiv 2 \bmod 3$ which contradicts the hypothesis. Therefore the result follows. ***(M1)(R1)(C1)(R1)***

(b) If $p \mid a$ then $p \mid a^2$ and since $p \mid a^2 + b^2$ then $p \mid (a^2 + b^2 - a^2)$ ***(R2)***

So, $p \mid b^2$. Since p is prime, p must divide b. ***(R1)***

(c) If $(a, b) = 1, \Rightarrow$ there are two integers s and r such that: $ra + sb = 1$, ***(M1)***

If $(a, c) = d, \Rightarrow$ there are two integers p and q such that: $pa + qc = d$, ***(M1)***

Then $pa + qc(ra + sb) = d$, and hence $(p + qcr)a + (qs)(bc) = d$ and hence the result follows. ***(M1)(R1)***

3. *[Maximum mark: 11]*

(a) The sum of the digits of a three-digit number of the form *abb* is divisible by 7. Show that the number itself is divisible by 7. *[4 marks]*

(b) Use Euclid's algorithm to find the smallest positive integers x and y that satisfy the equation $57x - 13y = 7$. *[7 marks]*

Solution

(a) The sum of the digits is divisible by $7 \Rightarrow \quad a + 2b \equiv 0 \mod 7$ *(M1)*

$abb = 100a + 10b + b$

$\equiv 100a + 11b \mod 7$ *(M1)*

$\equiv 2a + 4b \mod 7$ *(A1)*

$\equiv 2(a + 2b) \equiv 0 \mod 7$ *(C1)*

therefore *abb* is divisible by 7.

(b) gcd (57, 13) = 1 and we are going to apply Euclid's algorithm.

$$\left.\begin{array}{l} 57 = 13\times 4 + 5 \\ 13 = 5\times 2 + 3 \\ 5 = 3\times 1 + 2 \\ 3 = 2\times 1 + 1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} a = b\times 4 + r_1 \\ b = r_1\times 2 + r_2 \\ r_1 = r_2\times 1 + r_3 \\ r_2 = r_3\times 1 + r_4 \end{array}\right\} \Rightarrow \begin{array}{l} r_1 = a - 4b \\ r_2 = b - 2r_1 = 9b - 2a \\ r_3 = r_1 - r_2 = 3a - 13b \\ r_4 = r_2 - r_3 = 22b - 5a \end{array}$$ *(M1)* *(M1)*

Since $r_4 = 1$ we can find the particular solution. *(M1)*

$-5a + 22b = 1 \Rightarrow -35a + 154b = 7 \Rightarrow 57\times(-35) - 13\times(-154) = 7$ *(M1)*

So the particular solution is $(-35, -154)$. *(A1)*

Now the general solutions are given by the formula

$$\begin{cases} x = -35 + 13p \\ y = -154 + 57p \end{cases}, p \in \mathbb{Z}$$ *(M1)*

For $p = 3$ we get the smallest positive integers that are $x = 4$ and $y = 17$. *(A1)*

4. *[Maximum mark: 6]*

Show that the product of four consecutive integers is divisible by 24.

Solution

Three consecutive numbers are ≡0mod3, ≡1mod3, ≡2mod3.

Thus one of them is divisible by 3 and their product is divisible by 3

Four consecutive numbers are ≡0mod4, ≡1mod4, ≡2mod4, ≡3mod4.

Thus one of them is divisible by 4 and another one by 2. So their product is divisible by 8

Therefore, the product is divisible by 3×8=24.

5. *[Maximum mark: 5]*

Show that $n^4 + 4$ is not a prime for any $n > 1$, by using the binomial expansion of $(a + b)^2$

Solution

$n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 + 2n)(n^2 + 2 - 2n)$

Both factors are greater than 1 since

$(n^2 + 2 + 2n) = (n + 1)^2 + 1 > 1$

$(n^2 + 2 - 2n) = (n - 1)^2 + 1 > 1$, since $n > 1$.

6. *[maximum mark: 6]*

(a) Find the last digit of the number 2^{2017}

(b) Find $3^{1000} \bmod 7$ by using Fermat's little theorem.

Solution

(a) We can start from $2^{10} = 1024 \equiv 4 \bmod 10$

$2^{100} \equiv 4^{10} \equiv 6 \bmod 10$

$2^{1000} \equiv 6^{10} \equiv 6 \bmod 10$

$2^{2000} \equiv 6^2 \equiv 6 \bmod 10$

$2^{2017} \equiv 6 \times 2^{17} \equiv 2 \bmod 10$, so the last digit is 2

(b) $3^6 \equiv 1 \bmod 7$ by Fermat's little theorem.

$3^{6\times 166} = 3^{996} \equiv 1 \bmod 7$

$3^{1000} = 3^4 \equiv 4 \bmod 7$

7. *[maximum mark: 6]*

Solve $88x \equiv 1 \bmod 137$

Solution

Euclidean algorithm gives gdc(88,137) = 1 and $1 = 9 \times 137 - 14 \times 88$

The solution is $x \equiv -14 \bmod 137 = 123 \bmod 137$

8. *[maximum mark: 10]*

Solve

$$x \equiv 1 \bmod 2$$
$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$

(a) By the method of the proof of the Chinese remainder theorem.

(b) By setting $x = 2k + 1$ and similar substitutions.

Solution

The final answer is $x \equiv 23 \bmod 30$

9. *[maximum mark: 4]*

(a) Explain why the following system does not satisfy the conditions of the Chinese remainder theorem

$$x \equiv 5 \bmod 6$$
$$x \equiv 4 \bmod 5$$
$$x \equiv 3 \bmod 4$$
$$x \equiv 2 \bmod 3$$

(b) Show that it reduces to a system that satisfies these conditions. (Do not solve the system)

Solution

(a) 6,5,4,3 are not coprime

(b) $x \equiv 5 \bmod 6$ is equivalent to $x \equiv 2 \bmod 3$ and $x \equiv 1 \bmod 2$ and $x \equiv 3 \bmod 4$ implies $x \equiv 1 \bmod 2$

Thus the last 3 equations are enough.

10. *[maximum mark: 7]*

(a) Show that any integral power of 10 leaves a remainder of 1 when divided by 3. *[3 marks]*

It is given that any number $y \in \mathbb{N}$ can be written in expanded form as

$$y = a_n 10^n + a_{n-1} 10^{n-1} \ldots + a_1 10 + a_0$$

(b) Show that $y = 3k +$ sum of digits of y, for some $k \in \mathbb{N}$. *[3 marks]*

(c) Show that 3 divides y if 3 divides the sum of digits of y. *[1 mark]*

Solution

a) Since $10 = 9 + 1$ *(C1)*

then $10^n = \sum_0^n \binom{n}{i} 9^{n-i} = 9^n + n \times 9^{n-1} + \cdots + 9 + 1 = 3Q + 1, Q \in \mathbf{N}$ *(M1)(R1)*

Note: Some students may use mathematical induction, please award *(C3)*.

[3 marks]

b) $y = a_n(3k_n + 1) + a_{n-1}(3k_{n-1} + 1) + \cdots + a_1(3 \times 3 + 1) + a_0$ *(M1)*

$= 3(a_n k_n + a_{n-1} k_{n-1} + \cdots + a_1 \times 3) + a_n + a_{n-1} + \cdots + a_1 + a_0$ *(M1)*

$= 3k + a_n + a_{n-1} + \cdots a_1 + a_0$ *(R1)*

[3 marks]

c) If $3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$ then $3 \mid 3k + (a_n + a_{n-1} + \cdots + a_1 + a_0)$

and the result follows. *(R1)*

11. *[maximum mark: 5]*

The population of a village is 1100 people. Show that there are at least 4 people who share the same birthday.

Solution

Suppose that at most 3 people share the same birthday. So there are at most 3×366=1098 people, contradiction

12. *[maximum mark: 6]*

(a) If $p_1, p_2, p_3, \ldots, p_n$ are prime numbers of the form $4m + 3$, show that

$$s = 4p_1 p_2 p_3 \cdots p_n - 1$$

has a prime divisor of the form $4m + 3$.

(b) Show that there are infinitely many prime numbers of the form $4m + 3$.

Solution

(a) Notice that s is in fact of the form $4m + 3$

A prime number (when divided by 4) is either of the form $4m + 1$ or $4m + 3$.

Suppose that all prime divisors of s have the form $4m + 1$. But the product of two numbers of the form $4m + 1$ is also of the same form, since

$$(4m_1 + 1)(4m_2 + 1) = 4m_1(4m_2 + 1) + 4m_2 + 1 = 4(4m_1 m_2 + m_1 + m_2) + 1$$

Thus s is also of the form $4m + 1$, contradiction.

(b) Suppose that there are only n numbers of this form, namely $p_1, p_2, p_3, ..., p_n$
Then one of them, say p_k divides $s = 4p_1p_2p_3\cdots p_n - 1$ (by (a)). Thus p_k divides 1 as well (contradiction).

13. *[maximum mark: 6]*

Show that for any prime number p such that $n < p < 2n$

$$\text{(a) } \binom{2n}{n} \equiv 0 \bmod p. \qquad \text{(b) } \binom{2n}{n} \not\equiv 0 \bmod p^2$$

Solution

(a)

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{(n+1)(n+2)\cdots(2n)}{1\cdot 2\cdot 3\cdots n}$$

$$\Rightarrow 1\cdot 2\cdot 3\cdots n\binom{2n}{n} = (n+1)(n+2)\cdots(2n)$$

Clearly p divides the RHS, thus it divides the LHS. But p is coprime with $1\cdot 2\cdot 3\cdots n$, so it divides $\binom{2n}{n}$

(b) If p^2 divides $\binom{2n}{n}$, then p^2 also divides $(n+1)(n+2)\cdots(2n)$

But this is impossible since p is one of the factors and $p^2 > 2n$

14. *[maximum mark: 10]*

A sequence is defined recursively by

the first term	$u_1 = 10$
and the recursive relation	$u_{n+1} = 2u_n + 2$

(a) Given that the general solution is given by the formula $u_n = a(2)^n + b$, show that $a = 6$ and $b = -2$

(b) Prove by mathematical induction that $u_n = 6(2)^n - 2$, for $n \in \mathbb{Z}^+$

Solution

(a) $u_1 = 10$ and $u_2 = 22$

Hence

$10 = 2a + b$

$22 = 4a + b$

Therefore

$a = 6$ and $b = -2$

(b) Notice that the induction step is

$u_{k+1} = 2u_k + 2 = 2(6\times 2^k - 2) + 2 = 6\times 2^{k+1} - 4 + 2 = 6\times 2^{k+1} - 2$