

UNIVERSITY OF GLASGOW
DEPARTMENT OF MATHEMATICS
MATHEMATICS-2N

Number Theory Examples — Answers

1. 0, 6, -2, 5, -15, -3.
2. Let x and y be real numbers. Then $[x] \leq x$ and $[y] \leq y$. Therefore $[x] + [y] \leq x + y$. But $[x] + [y]$ is an integer and $[x + y]$ is the *greatest* integer less than or equal to $x + y$. Hence $[x] + [y] \leq [x + y]$.
 $x = y = \frac{1}{2}$.
3. No, $x = y = -\frac{1}{2}$.
4. Suppose that $x \in \mathbb{Z}$. Then $[x] + [-x] = x + (-x) = 0$.
Now suppose that $x \notin \mathbb{Z}$. Then $[x] < x < [x] + 1$. Therefore $-[x] - 1 < -x < -[x]$. So $-[x] - 1$ is the greatest integer less than or equal to $-x$, i.e. $[-x] = -[x] - 1$.

$$\therefore [x] + [-x] = -1.$$

5. (i) $q = 4, r = 2$; (ii) $q = 5, r = 0$; (iii) $q = 0, r = 7$; (iv) $q = -5, r = 6$.
6. (i) $q = -4, r = 3$; (ii) $q = 5, r = 2$.
7. $(3422312)_5, (EE1D)_{16}$.
8. $b = au$ and $c = bv$ for some integers u, v . So $c = auv$, where uv is an integer. $\therefore a|c$.
9. $a = 4, b = c = 2$.
10. $b = au$ and $a = bv$ for some integers u, v . So $a = auv$. If $a = 0$ then clearly $b = 0$, in particular $a = b$. Now assume that $a \neq 0$. Then $uv = 1$. So $v = \pm 1$, i.e. $a = \pm b$.
Alternative solution for the case $a, b \neq 0$. $|a| \leq |b|$ and $|b| \leq |a|$. So $|a| = |b|$, i.e. $a = \pm b$.
11. Assume that $a|b$. Then $b = au$ for some integer u . $\therefore nb = nau$. $\therefore na|nb$.
Conversely, assume that $na|nb$. Then $nb = nau$ for some integer u . Since $n \neq 0$, $b = au$. $\therefore a|b$.
12. $c = abu$ for some integer u . Since bu is an integer, $a|c$. Since $c = bau$ and au is an integer, $b|c$.
 $a = b = c = 2$.
13. $b = au$ and $d = cv$ for some integers u, v . So $bd = acuv$ and uv is an integer. $\therefore ac|bd$.
14. Two consecutive integers have the form $2q, 2q + 1$ or $2q + 1, 2q + 2$ for some integer q and product $2q(2q + 1)$ or $(2q + 1)(2q + 2) = 2(2q + 1)(q + 1)$. So the product is even.
Let a be an odd integer. Then $a = 2k + 1$ for some integer k .

$$\therefore a^2 - 1 = (2k + 1)^2 - 1 = 4k(k + 1).$$

Being the product of two consecutive integers, $k(k + 1)$ must be even. So $k(k + 1) = 2u$ for some integer u . $\therefore a^2 - 1 = 8u$. $\therefore 8|(a^2 - 1)$.

15. Let $d = \gcd(15a + 1, 13a - 2)$ for some integer a . Then $d \mid (15a + 1)$ and $d \mid (13a - 2)$.

$$\therefore d \mid (13(15a + 1) - 15(13a - 2)), \text{ i.e. } d \mid 43.$$

$$\therefore d = 1 \text{ or } d = 43 \text{ since } d > 0.$$

16. Let $d = \gcd(39a + 5, 26a - 1)$ for some integer a . Then $d \mid (39a + 5)$ and $d \mid (26a - 1)$.

$$\therefore d \mid (2(39a + 5) - 3(26a - 1)), \text{ i.e. } d \mid 13.$$

$$\therefore d \mid (2a(13) - 1(26a - 1)), \text{ i.e. } d \mid 1.$$

$$\therefore d = 1 \text{ since } d > 0.$$

17. 53; $-53, -1, 1, 53$; $x = -4, y = 3$.

18. $x = -31 + 97t, y = 8 - 25t$ ($t \in \mathbb{Z}$).

19. $x = -195 + 161t, y = 63 - 52t$ ($t \in \mathbb{Z}$); $x = 63 - 52t, y = 195 - 161t$ ($t \in \mathbb{Z}$);
 $x = 115, y = 356$; $x = 63, y = 195$; $x = 11, y = 34$.

20. $x = 2, y = 3$.

21. $\gcd(51, 85) = 17$ and $17 \nmid 100$.

22. $x = 3500 + 16t, y = -5000 - 23t$ ($t \in \mathbb{Z}$); one, namely $x = 12, y = 14$.

23. 57. (Let x be the number of students and y the number of other people present. Then $150x + 360y = 18000$ and $y > 2x > 0$, i.e. $x = 12, y = 45$.)

24. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. So $nd \mid na$ and $nd \mid nb$ by Example 11, i.e. nd is a common divisor of na and nb . Therefore $0 < nd \leq \gcd(na, nb)$. Also $ax + by = d$ for some integers x, y . But then $nax + nby = nd$. So $\gcd(na, nb) \mid nd$ by the condition for a Diophantine equation to have an integral solution. Therefore $\gcd(na, nb) \leq nd$. Hence $\gcd(na, nb) = nd$, i.e. $\gcd(na, nb) = n \gcd(a, b)$.

25. $c = au$ and $c = bv$ for some integers u, v . Also, we can find integers x, y such that $ax + by = 1$.

$$\therefore c = (ax + by)c = axc + byc = axbv + byau = ab(xv + yu).$$

Since $xv + yu$ is an integer, $ab \mid c$.

26. $ax + cy = 1$ and $bz + ct = 1$ for some integers x, y, z, t . So

$$(ax + cy)(bz + ct) = 1,$$

$$\text{i.e. } abxz + c(axt + byz + c yt) = 1.$$

Since xz and $axt + byz + c yt$ are integers, $\gcd(ab, c) \mid 1$. So $\gcd(ab, c) = 1$, i.e. ab and c are coprime.

The result is true for $n = 3$ by the first part.

Now assume, inductively, that the result is true for $n = k$ ($k \geq 3$). Suppose we are given pairwise coprime integers $m_1, m_2, \dots, m_k, m_{k+1}$. By the induction hypothesis applied to $m_1, m_2, \dots, m_{k-1}, m_{k+1}$, we have $m_1 m_2 \dots m_{k-1}$ and m_{k+1} are coprime. Then, by the first part, $m_1 m_2 \dots m_{k-1} m_k$ and m_{k+1} are coprime, i.e. the result is also true for $n = k + 1$.

By induction, the result is true for all integers $n \geq 3$.

27. If $m_1 m_2 \dots m_n | c$ then $m_i | c$ ($i = 1, 2, \dots, n$) by Example 12.

To prove the converse by induction, let $S(n)$ be the statement: if m_1, m_2, \dots, m_n are pairwise coprime integers and $m_i | c$ ($i = 1, 2, \dots, n$) then $m_1 m_2 \dots m_n | c$. $S(n)$ is true for $n = 2$ by Example 25.

Now assume, inductively, that $S(n)$ is true for $n = k$ ($k \geq 2$). Suppose that m_1, m_2, \dots, m_{k+1} are pairwise coprime integers and $m_i | c$ ($i = 1, 2, \dots, k+1$). Then $m_1 m_2 \dots m_k$ and m_{k+1} are coprime by Example 26 and $m_1 m_2 \dots m_k | c$ by the induction hypothesis. But $m_{k+1} | c$ as well; so $m_1 m_2 \dots m_k m_{k+1} | c$ by Example 25. Therefore $S(n)$ is also true for $n = k + 1$.

Hence, by induction, $S(n)$ is true for all integers $n \geq 2$.

28. $x = -49, y = -49, z = 49$;

$$x = -49 + 13t, \quad y = -49 + 12t + 3s, \quad z = 49 - 12t - 2s \quad (s, t \in \mathbb{Z}).$$

29. (i) Prime, (ii) $111 = 3.37$, (iii) $1111 = 11.101$, (iv) $1001 = 7.143$, (v) $11111 = 41.271$.

30. 6.

31. $2^3.3.7^2.13.19$.

32. (i) $ab = \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i}$. So, by the uniqueness of expressions as products of primes,

$$ab = c \iff \alpha_i + \beta_i = \gamma_i \quad (i = 1, 2, 3, \dots).$$

(ii) Assume that $a | b$. Then $b = au$ for some positive integer u . But $u = \prod_{i=1}^{\infty} p_i^{\nu_i}$ for some non-negative integers ν_i ($i = 1, 2, 3, \dots$) and, by part (i), $\alpha_i + \nu_i = \beta_i$ ($i = 1, 2, 3, \dots$). So $\alpha_i \leq \beta_i$ ($i = 1, 2, 3, \dots$).

Conversely, assume that $\alpha_i \leq \beta_i$ ($i = 1, 2, 3, \dots$). Let $\nu_i = \beta_i - \alpha_i$ ($i = 1, 2, 3, \dots$) and let $u = \prod_{i=1}^{\infty} p_i^{\nu_i}$. Then $\beta_i = \alpha_i + \nu_i$ ($i = 1, 2, 3, \dots$) and $b = au$ by part (i). So $a | b$.

(iii) Let $d = \prod_{i=1}^{\infty} p_i^{\delta_i}$, with δ_i ($i = 1, 2, 3, \dots$) non-negative integers. Then, by part (ii), d is a common divisor of a and b if and only if $\delta_i \leq \alpha_i$ and $\delta_i \leq \beta_i$ ($i = 1, 2, 3, \dots$). So d is the greatest common divisor of a and b provided $\delta_i = \min(\alpha_i, \beta_i)$ ($i = 1, 2, 3, \dots$).

(iv) Let $m = \prod_{i=1}^{\infty} p_i^{\mu_i}$, with μ_i ($i = 1, 2, 3, \dots$) non-negative integers. Then, by part (ii), m is a common multiple of a and b if and only if $\alpha_i \leq \mu_i$ and $\beta_i \leq \mu_i$ ($i = 1, 2, 3, \dots$). So m is the least common multiple of a and b provided $\mu_i = \max(\alpha_i, \beta_i)$ ($i = 1, 2, 3, \dots$).

33. In the notation of Example 32,

$$\gcd(a, b)\text{lcm}(a, b) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)}, \quad ab = \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i}.$$

But $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$ ($i = 1, 2, 3, \dots$). Hence

$$\gcd(a, b)\text{lcm}(a, b) = ab.$$

$$\text{lcm}(4655, 12075) = 1605975.$$

34. 2, 6, 10, 14, 18, 22.

Adapt the proof of Theorem 8 to show that every positive member of E can be expressed as a product of E -primes.

$$36 = 6.6 = 2.18, \quad 60 = 6.10 = 2.30.$$

35. Assume that $2^n - 1$ is prime for some positive integer n . The divisors of $2^{n-1}p$, where $p = 2^n - 1$, other than itself are $1, 2, 2^2, \dots, 2^{n-1}, p, 2p, 2^2p, \dots, 2^{n-2}p$, and

$$\begin{aligned} 1 + 2 + 2^2 + \dots + 2^{n-1} + p + 2p + 2^2p + \dots + 2^{n-2}p &= \frac{1(1 - 2^n)}{1 - 2} + \frac{p(1 - 2^{n-1})}{1 - 2} \\ &= p - p(1 - 2^{n-1}) \\ &= 2^{n-1}p. \end{aligned}$$

Hence $2^{n-1}p$, i.e. $2^{n-1}(2^n - 1)$, is a perfect number.

$n = 7$ gives the perfect number 8128.

36. 6, 4.

37. Let p be a prime greater than 3. Then $p = 6k \pm 1$ for some positive integer k . So $p^2 - 1 = 36k^2 \pm 12k = 24k^2 + 12k(k \pm 1)$. Being a product of consecutive integers, $k(k \pm 1) = 2u$ for some integer u (see Example 14). Hence

$$p^2 - 1 = 24k^2 + 24u = 24(k^2 + u)$$

and $k^2 + u$ is an integer. Therefore $p^2 \equiv 1 \pmod{24}$.

38. (i) True (Prop. 9.2(ii)),
 (ii) false (counter-example: $a = 0, b = 1, m = 2$),
 (iii) false (counter-example: $a = 0, b = 2, m = 2$),
 (iv) true (assume that $a \equiv b \pmod{2m}$; then $a - b = 2mu$ for some integer u , i.e. $a - b = m2u$, and so $a \equiv b \pmod{m}$ since $2u$ is an integer).

39. $a - b = mu$ for some integer u . Now $a = 1b + um$. So every common divisor of b and m is a divisor of a by Theorem 1. Also $b = 1a + (-u)m$. So every common divisor of a and m is a divisor of b . Therefore a and m have the same common divisors as b and m . In particular, $\text{gcd}(a, m) = \text{gcd}(b, m)$.

40. (Prop. 9.3)

41.

+	0	1	2	3	4	5	6	7	8	9	0	×	0	1	2	3	4	5	6	7	8	9	
0	0	1	2	3	4	5	6	7	8	9	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	2	3	4	5	6	7	8	9	0	1	1	0	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1	2	2	0	2	4	6	8	0	2	4	6	8	0
3	3	4	5	6	7	8	9	0	1	2	3	3	0	3	6	9	2	5	8	1	4	7	0
4	4	5	6	7	8	9	0	1	2	3	4	4	0	4	8	2	6	0	4	8	2	6	0
5	5	6	7	8	9	0	1	2	3	4	5	5	0	5	0	5	0	5	0	5	0	5	0
6	6	7	8	9	0	1	2	3	4	5	6	6	0	6	2	8	4	0	6	2	8	4	0
7	7	8	9	0	1	2	3	4	5	6	7	7	0	7	4	1	8	5	2	9	6	3	0
8	8	9	0	1	2	3	4	5	6	7	8	8	0	8	6	4	2	0	8	6	4	2	0
9	9	0	1	2	3	4	5	6	7	8	9	9	0	9	8	7	6	5	4	3	2	1	0

$2 \equiv 3.4, \quad 3 \equiv 7.9, \quad 4 \equiv 2.2, \quad 5 \equiv 5.7, \quad 6 \equiv 2.3, \quad 7 \equiv 3.9, \quad 8 \equiv 2.4, \quad 9 \equiv 3.3 \pmod{10}$. So there are no primes modulo 10 and consequently factorisation modulo 10 is not unique.

45. 17654212521 is divisible by 3, 9 and 11; 15023567847 is divisible by 3 but not by 9 or 11.
46. (i) $x \equiv 13 \pmod{17}$, (ii) $x \equiv 3 \pmod{9}$, (iii) $x \equiv 17 \pmod{19}$.
47. (i) $x \equiv 69 \pmod{110}$, (ii) $x \equiv 76 \pmod{168}$, (iii) $x \equiv 173 \pmod{210}$.
48. $x \equiv 331 \pmod{468}$.
49. $x \equiv 51 \pmod{110}$.
50. (i) No (the set has only 5 members, there is nothing congruent to 0 (mod 6)),
(ii) no ($15 \equiv 3 \pmod{6}$, there is nothing congruent to 5 (mod 6)),
(iii) yes (it is a set of 6 incongruent integers (mod 6)),
(iv) no (the set has 7 members, $17 \equiv 11 \pmod{6}$),
(v) yes! (it is a set of 6 incongruent integers (mod 6)).
51. (i) 32, (ii) 36, (iii) 144.
52. (i) 8, (ii) 720, (iii) 720.
55. The integers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 which are coprime with 12 are 1, 5, 7, 11.
(i) No ($17 \equiv 29 \pmod{12}$, there is nothing congruent to 7 (mod 12)),
(ii) no ($15 \equiv 3 \pmod{12}$, which is not coprime with 12, there is nothing congruent to 11 (mod 12)),
(iii) yes (the set has 4 members which are variously congruent to 1, 5, 7, 11 (mod 12)),
(iv) no (the set has only 3 members, there is nothing congruent to 5 (mod 12)).
56. 6.
57. (i) $3^{17} \equiv 5 \pmod{7}$, (ii) $3^{17} \equiv 3 \pmod{8}$, (iii) $40^{60} \equiv 1 \pmod{61}$,
(iv) $7^{1014} \equiv 8 \pmod{31}$, (v) $5^{1166} \equiv 4 \pmod{41}$.
59. Yes, all odd positive integers.

60. Let m be a positive integer. Two integers which have the same remainder upon division by m differ by a multiple of m . Hence the integers in a set of m consecutive integers have m different remainders. But there are only m possible remainders: 0, 1, \dots , $m - 1$. Therefore exactly one element in such a set has remainder 0, i.e. exactly one element is divisible by m .

Alternative solution. Let a be the least integer in a set S of m consecutive integers, where m is a positive integer. Then $a = qm + r$ for some integers q, r such that $0 \leq r < m$, and $a + m - r = (q + 1)m$. If $r = 0$ then a is divisible by m . If $r > 0$ then $a + m - r$ belongs to S and is divisible by m . S cannot have two elements divisible by m because no two elements of S differ by a multiple of m .

(i) Let n be an integer greater than 2. One of the 3 consecutive integers $2^n - 1, 2^n, 2^n + 1$ is divisible by 3. Clearly 2^n is not divisible by 3 since factorisation as a product of primes is unique. So either $2^n - 1$ or $2^n + 1$ is divisible by 3. Since it is greater than 3, the one divisible by 3 cannot be prime.

(ii) Let a be any integer. Then

$$a^5 - 5a^3 + 4a = (a + 2)(a + 1)a(a - 1)(a - 2).$$

One of the 5 consecutive integers $a + 2, a + 1, a, a - 1, a - 2$ is divisible by 5, at least one is divisible by 4 and at least one is divisible by 3. So $a^5 - 5a^3 + 4a$ is divisible by 5, 4 and 3. Since 5, 4 and 3 are pairwise coprime, $a^5 - 5a^3 + 4a$ is divisible by $5 \cdot 4 \cdot 3$. But $5 \cdot 4 \cdot 3 = 60$. Hence $a^5 - 5a^3 + 4a \equiv 0 \pmod{60}$.

61. (i) $n = 2^\alpha$ ($\alpha \in \mathbb{N}$), (ii) $n \equiv 0 \pmod{3}$ ($n > 0$), (iii) $n = 13, 21, 26, 28, 36$ or 42 .
62. $\text{ord}_{13}a = 1, 12, 3, 6, 4, 12, 12, 4, 3, 6, 12, 12$ when $a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$, respectively.