THE UNIVERSITY OF SYDNEY
SCHOOL OF MATHEMATICS AND STATISTICS

Solutions to Number Theory and O-Notation – Week 6 Tutorials

MATH1064: Discrete Mathematics for Computing

1. Prove that for all $x \in \{0,1,2,3,4\}$, x^2+x+41 is a prime number.

Solution: Exhaustion — try all cases. Try larger values if you don't find it exhausting! This is called Euler's polynomial, and every $x \in \{n \in \mathbb{N} \mid 0 \le n \le 39\}$ will give you a prime number. Can you see why $x = 40$ and $x = 41$ give composite numbers?

2. Prove the following statement by contradiction. For all integers n and all prime numbers p, if n^2 is divisible by p, then n is divisible by p.

Solution: Contraposition: Assume n is not divisible by p. Then by uniqueness of prime factorisation, n^2 is not divisible by p.

3. Write each of the following integers as a product of primes. Don't use a calculator!

(a) 5440 (b) 43560 (c) 44352

Solution: $5440 = 2^6 \cdot 5 \cdot 17$

Solution: $43560 = 2^3 \cdot 3^2 \cdot 5 \cdot 11^2$

Solution: $44352 = 2^6 \cdot 3^2 \cdot 7 \cdot 11$

4. Given the following values for n and d, find integers q and r such that $n = d \cdot q + r$ and $0 \le r < d$.

(a) $n = 102$ and $d = 11$

Solution: $102 = 11 \cdot 9 + 3$, so $q = 9$ and $r = 3$

(b) $n = -4$ and $d = 5$

Solution: $-4 = 5 \cdot (-1) + 1$, so $q = -1$ and $r = 1$

(c) $n = 200$ and $d = 71$

Solution: $200 = 71 \cdot 2 + 58$, so $q = 2$ and $d = 58$

5. (a) Find $gcd(m,n)$, where $m = 2^3 \cdot 3^2 \cdot 5 \cdot 11^2$ and $n = 2 \cdot 3^2 \cdot 11 \cdot 13^2$.

Solution: $gcd(m,n) = 2 \cdot 3^2 \cdot 11$.

(b) A positive integer is called squarefree if it is not divisible by the square of any prime. What can you deduce about the factorisation of a squarefree number into distinct primes?

Solution: All the exponents of the factorisation have to be equal to one, i.e. the integer $n = p_1 \cdots p_n$ where the p_i are distinct primes.

(c) Show that every positive integer can be expressed as a product of a squarefree integer and a square number.

Solution: Let n be a positive integer. By the fundamental theorem we can factor n into distinct primes: $n = p_1^{a_1} \cdots p_n^{a_n}$. Write each $a_i = 2k_i + \delta_i$, where δ_i is either 0 or 1 depending on whether a_i is even or odd. Let $s = p_1^{2k_1} \cdots p_n^{2k_n}$ and $t = p_1^{\delta_1} \cdots p_n^{\delta_n}$. Then we have $n = st$. Further, note that s is a square number since $\sqrt{s} = p_1^{k_1} \cdots p_n^{k_n}$, and t is squarefree.

6. Use the Euclidean algorithm to find

(a) $\gcd(101, 100)$. (b) $\gcd(123, 277)$. c) $\gcd(14039, 1529)$.

Solution:

$a = 101, b = 100$.
Sequence of remainders: $1, 0$,
$\gcd(101, 100) = 1$

Solution:

$a = 277, b = 123$.
Sequence of remainders: $31, 30, 1, 0$,
$\gcd(277, 123) = 1$

Solution:

$a = 14039, b = 1529$.
Sequence of remainders: $278, 139, 0$,
$\gcd(14039, 1529) = 139$

7. (More difficult) Prove or disprove the following statement.

$$\forall a, b \in \mathbb{Z}, \big(\ (\gcd(a,b) = r) \ \rightarrow\ (\exists x, y \in \mathbb{Z} \text{ such that } r = ax + by)\ \big)$$

Solution: This is called Bézout's identity.

Proof 1: run the extended Euclidean algorithm, see

`https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm`

Proof 2: Here is a proof without using the Euclidean algorithm.

Suppose $a, b \in \mathbb{Z}$ and $r = \gcd(a, b)$.

Define $D = \{k \mid k = ax + by, x, y \in \mathbb{Z}, k > 0\}$.

Let c be the smallest element of D. This exists since all elements of D are positive integers.

We now use the definition of $\gcd(a, b)$ to show that r divides c and so $r \leq c$.

Namely, $a = rn$ and $b = rm$ for some $n, m \in \mathbb{Z}$. Since $c \in D$, we have $c = ax + by$ for some $x, y \in \mathbb{Z}$. Hence $c = rnx + rmy = r(nx + my)$, and so r divides c. Hence $r \leq c$.

We next show that $r \geq c$. For this, do division with remainder. To get started, note that $|a| \in D$ and $|b| \in D$. This follows from choosing x (or y) equal to zero and y (or x) equal to ± 1, depending on whether a (or b) is positive or negative. This implies that $c \leq |a|$ and $c \leq |b|$.

So we can write $a = qc + s$, where $q, s \in \mathbb{Z}$ and $0 \leq s < c$. Since $c = ax + by$, we have $a = q(ax + by) + s$ and so $s = a(1 - qx) - bqy$. If $s > 0$, we have $s \in D$. But $s < c$ and c is the smallest element in D, a contradiction Hence $s = 0$. Hence c divides a.

By a similar argument, c divides b. So c divides both a and b and hence $c \leq r$.

So we have shown that $c \leq r$ and $c \geq r$. This implies $c = r$. The upshot is that $r \in D$ and hence the statement is true.

8. Convert the decimal expansion of each of these integers to a binary expansion.

(a) 231 (b) 321 (c) 1023

Solution:

(a) $(11100111)_2$
(b) $(101000001)_2$
(c) $(1111111111)_2$

9. Convert the binary expansion of each of these integers to a decimal expansion.

(a) $(11111)_2$ (b) $(1000000001)_2$ (c) $(101010101)_2$

Solution:

(a) 31
(b) 513
(c) 341

10. Convert the hexadecimal expansion of each of these integers to a binary expansion.

(a) $(80E)_{16}$ (b) $(135AB)_{16}$ (c) $(ABBA)_{16}$

Solution: All you need to do is translate every hexadecimal letter into a 4-digit binary number (i.e., $A \mapsto 1010$) and concatenate the result.

(a) $(100000001110)_2$
(b) $(10011010110101011)_2$
(c) $(1010101110111010)_2$

11. Find the sum and the product of each of these pairs of numbers. Express your answers as a binary expansion.

(a) $(111)_2$, $(101)_2$

Solution:

Sum: $(1100)_2$
Product: $(100011)_2$

(b) $(1110)_2$, $(1010)_2$

Solution:
Sum: $(1\,1000)_2$
Product: $(1000\,1100)_2$

(c) $(10\,1010\,1010)_2$, $(10)_2$

Solution:
Sum: $(10\,1010\,1100)_2$
Product: $(101\,0101\,0100)_2$

12. Let $f(n) = n^2 + n$ and $g(n) = \frac{1}{2}n^3$.
Use the definition of O–notation to show that $f(n) \in O(g(n))$ but $g(n) \notin O(f(n))$.

Solution: First note that $f(n) > 0$ and $g(n) > 0$ for all $n \in \mathbb{N}$. We therefore don't need to take absolute values of the functions involved.

We have $n^2 + n \leq n^3 + n^3 = 2n^3 = 4 \cdot (\frac{1}{2}n^3)$ for all $n > 1$, hence $f(n) \in O(g(n))$.

The second statement is shown by contradiction. Suppose $g(n) \in O(f(n))$. Then there are witnesses C and k such that $g(n) \leq Cf(n)$ for all $n > k$.

Hence $\frac{1}{2}n^3 = g(n) \leq f(n) = n^2 + n$ for all $n > k$.

This implies $\frac{1}{2}n^2 \leq n + 1$ for all $n > k$.

Now $n + 1 \leq n + n = 2n$ for all $n > 0$, and so we have

$\frac{1}{2}n^2 \leq 2n$ for all $n > \max(0,k)$.

This implies $\frac{1}{2}n \leq 2$ for all $n > \max(0,k)$, and therefore $n \leq 4$ for all $n > \max(0,k)$. But this is a contradiction. Hence $g(n) \notin O(f(n))$.

13. Let c be a constant. Multiply $(\log(n) + c + O(1/n))$ by $(n + O(\sqrt{n}))$ and express your answer in O–notation.

Solution: Answer: $n\log(n) + cn + O(\sqrt{n}\log(n))$

14. True or false? If $f(n)$ and $g(n)$ are positive for all $n \in \mathbb{N}$, then

$$O(f(n) + g(n)) = f(n) + O(g(n)).$$

If true give a proof; if false, give a counterexample.

Solution: Let $f(n) = n^2$, $g(n) = 1$ and $h(n) = n$. Then $h(n) \in O(f(n) + g(n))$ but $h(n) \notin f(n) + O(g(n))$.