Number theory: Problem sheet 1

Solutions to indicated problems must be submitted by Monday 4 November 2013
You are encouraged to submit solutions to non-assessed problems too

1. (A) Remind yourself of the Sieve of Eratosthenes, or look it up if you are unfamiliar with it. Use it to find all primes up to 200.

   (If you like programming, write a programme to find all primes up to 1000 or beyond!)

2. (A) In each case, using the extended Euclidean algorithm in full, find $g = \gcd(a, b)$ and find integers r and s such that $g = ra + sb$:

   (i) $a = 315$, $b = 119$;
   (ii) $a = 777$, $b = 434$;
   (iii) $a = 2013$, $b = 1804$. [(iii) 5 marks]

   (Again, if you like programming, write a programme to implement the extended Euclidean algorithm, and try it on some really large numbers.)

3. (A) Prove that the Diophantine equation

   $$x^2 - 71y^2 = -1$$

   has no solutions with x, $y \in \mathbf{Z}$. [10 marks]

4. (A) Recall that if the two numbers m and n are coprime, then there are integers r and s with $rm + sn = 1$. Let's look at similar problems with *three* numbers.

   (i) Find integers r, s and t with $6r + 14s + 21t = 1$.
   (ii) Find integers r, s and t with $55r + 65s + 143t = 1$. [(ii) 5 marks]

   (Note that no pair of the numbers 6, 14 and 21 are coprime, so in (i) all of r, s and t must be nonzero.)

5. (A) The Fibonacci numbers $(F_n)_{n=1}^{\infty}$ are defined recursively by $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$. Write down F_n for all n up to 15.

   Prove, by induction or otherwise, that $\gcd(F_{n+1}, F_n) = 1$ for all n.

   (As a followup, you might like to investigate how $\gcd(F_m, F_n)$ depends on m and n.)

6. (B) (Number of steps in Euclidean algorithm.)

   In the Euclidean algorithm applied to numbers m and n, we start with $n_1 = m$ and $n_2 = n$ and produce a sequence of numbers n_1, n_2, $n_3, \ldots$ ending when we get to some n_k with $n_k \mid n_{k-1}$. Prove that when $r \geq 2$ then either $n_{r+1} \leq n_r/2$ or that $n_{r+2} \leq n_r/2$. Conclude that $k \leq 2 + 2\log_2 n$. [10 marks]

7. (A) Find the prime factorizations of each of the following numbers:

   (i) 108; (ii) 15120; (iii) 15180; (iv) 111111.

8. (A) Prove that the least prime factor p of a composite number n satisfies $p \leq \sqrt{n}$.

9. (B) Prove that there are infinitely many prime numbers p satisfying $p \equiv 5 \pmod 6$.

10. (B) For the purposes of this question, a *nice number* is an integer ending in 3 or 7 when written out in decimal. Prove that every nice number has a prime factor that is also a nice number. Deduce that there are infinitely many nice prime numbers. [20 marks].

11. (A) Let $n \in \mathbf{N}$ with $n \geq 2$. Consider the numbers $n!+2, n!+3, \ldots, n!+n$. Show that none of them is prime. Deduce that for each positive integer N there is a stretch of N consecutive composite numbers. [10 marks]

12. (B) Let $n = p^e q^f$ where p and q are distinct primes and e and f are positive integers. Show that n has $(e+1)(f+1)$ distinct factors in $\mathbf{N}$, and that the sum of all these factors is

$$\frac{(p^{e+1}-1)(q^{f+1}-1)}{(p-1)(q-1)}.$$

    (You may assume the uniqueness of prime factorization). [20 marks]

    What if n has more than two distinct prime factors?

    (Hint: you may wish to warm up by doing $n = p^e$ first.)

13. (B) (This exercise aims to show that uniqueness of prime factorization is not obvious.)

    Let

$$A = \{1, 11, 21, 31, 41, \ldots\} = \{10n - 9 : n \in \mathbf{N}\}$$

    be the set of natural numbers whose base-ten representations end in 1.

Show that A is closed under multiplication: that is, if $a \in A$ and $b \in A$ then $ab \in A$.

We say that an element a of A is an *A-prime* if $a > 1$ and a isn't the product of two smaller elements of A. Show that if $a \in A$ and $a > 1$ then either a is an A-prime or that a is a product of A-primes.

By considering the number $29241 = 171^2$, or otherwise, show that factorization of elements of A into A-primes is not always unique.

What goes wrong if you try to adapt the proof of unique prime factorization to prove the uniqueness of A-prime factorization?

14. (A) Prove that $a \equiv b \pmod{n}$ if and only if $ma \equiv mb \pmod{mn}$. (Here, a, $b \in \mathbf{Z}$ and m, $n \in \mathbf{N}$.)

15. (A) Solve the following linear congruences (that is, find the general solution, or prove that no solution exists):

    (i) $8x \equiv 9 \pmod{19}$;

    (ii) $77x \equiv 62 \pmod{105}$;

    (iii) $57x \equiv 48 \pmod{135}$;

    (iv) $67x \equiv 282 \pmod{283}$; [(iv) 5 marks]

    (v) $737x \equiv 1727 \pmod{2002}$. [(v) 5 marks]

16. (A) Solve, whenever possible, each of the following systems of simultaneous congruences:

    (i) $x \equiv 4 \pmod{13}$, $x \equiv 12 \pmod{17}$;

    (ii) $x \equiv 11 \pmod{22}$, $x \equiv 3 \pmod{40}$;

    (iii) $x \equiv 71 \pmod{112}$, $x \equiv 111 \pmod{189}$; [(iii) 5 marks]

    (iv) $19x \equiv 11 \pmod{31}$, $23x \equiv 57 \pmod{61}$;

    (v) $x \equiv 10 \pmod{11}$, $x \equiv 5 \pmod{12}$, $x \equiv 1 \pmod{13}$. [(v) 5 marks]

17. (C) Prove that if $n \in \mathbf{N}$ and $n \geq 2$ then $n^4 + 4^n$ is composite.

RJC 26/9/2013