

Number theory: Problem sheet 1

Solutions must be submitted by Thursday 24 February 2005

1. Visit and bookmark the course webpage:

<http://www.maths.ex.ac.uk/~rjc/courses/nt04/nt04.html> . [1]

2. Use the sieve of Eratosthenes to find all primes up to 200. [10]

3. 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) $a = 93, b = 69$;

(ii) $a = 665, b = 411$;

(iii) $a = 2005, b = 1066$.

[9]

4. In each case, using the `igcd` command in MAPLE find $g = \gcd(a, b)$:

(i) $a = 2^{32} - 1, b = 2^{24} - 1$;

(ii) $a = 10^{24} - 1, b = 8^{24} - 1$;

(iii) $a = 123456789012345678901, b = 103679376657667651069$.

[9]

5. 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 $55r + 65s + 143t = 1$.

[10]

6. 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, that $\gcd(F_{n+1}, F_n) = 1$ for all n . [13]

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

7. Find the prime factorizations of each of the following numbers:

(i) 102; (ii) 720; (iii) 1001; (iv) 19380.

For each of these numbers n , write down $v_p(n)$ for *all* primes p . (Recall that $v_p(n)$ is the integer e such that $p^e \mid n$ but $p^{e+1} \nmid n$.) [12]

8. Let $n \in \mathbf{N}$ with $n \geq 2$. Consider the numbers $n! + 2, n! + 3, \dots, n! + n$. Show that none of them is prime, and deduce that there are arbitrarily long finite stretches of consecutive composite numbers in $\mathbf{N}$. [8]

9. Let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

be the prime factorization of some number $n \in \mathbf{N}$ (we assume in this notation that $p_1, \dots, p_k$ are all distinct). Show that n has

$$\prod_{j=1}^k (e_j + 1)$$

distinct divisors in $\mathbf{N}$, and that the sum of all these divisors is

$$\prod_{j=1}^k \frac{p_j^{e_j+1} - 1}{p_j - 1}.$$

[16]

(Hint: if you cannot see how to do the general case immediately, try some special cases, e.g., when $n = p_1^{e_1}$ is a prime power or when $n = p_1 p_2 \cdots p_k$ is a product of distinct primes).

10. (This exercise aims to show that uniqueness of prime factorization is not obvious.

Let

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

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. [12]

11. (Challenge problem). Show that if $n \in \mathbf{N}$ and $n \geq 2$ then $n^4 + 4^n$ is composite.