Michaelmas Term 2012 J. M. E. Hyland

Number Theory: Example Sheet 1

The first 12 questions are intended for the supervisions. Further questions are designed to encourage mathematical investigation without any examination emphasis.

1. Calculate $d = (a, b)$ and find integers x and y such that $d = ax + by$ when

   (i) $a = 841$, $b = 160$; (ii) $a = 2613$, $b = 2171$.

2. Let a and b be integers with $a \geqslant b \geqslant 1$. Let $\lambda(a, b)$ be the number lines in Euclid's algorithm to compute (a, b) not counting the line with remainder 0. Prove that

   $$\lambda(a, b) \leqslant 2 \left\lfloor \frac{\log b}{\log 2} \right\rfloor .$$

   (Notation: the *floor function* $\lfloor x \rfloor$ of a real number x is the largest integer less than or equal to x.)

3. Let x be an integer greater than 1. By considering the Fundamental Theorem of Arithmetic show that

   $$x \leqslant \left(1 + \frac{\log x}{\log 2}\right)^{\pi(x)} .$$

   Hence deduce that when $x \geqslant 8$ we have $\pi(x) \geqslant \dfrac{\log x}{2 \log \log x}$.
   (Notation: the function $\pi(x)$ of a real number x is the number of primes less than or equal to x.)

4. By considering numbers of the form $n = 2^2 \cdot 3 \cdot 5 \cdot \cdots \cdot p - 1$, prove that there are infinitely many primes congruent to 3 mod 4.

5. Let a and n be integers greater than 1. Prove that if $a^n - 1$ is prime, then a must be 2 and n must be prime. Without considering the next question is the converse plausible?

6. Let q be an odd prime.
   (i) Prove that every prime factor of $2^q - 1$ must be congruent to 1 mod q.
   (ii) Prove that every prime factor of $2^q - 1$ must be congruent to ± 1 mod 8.

   Use the above results to factor $2^{11} - 1 = 2047$.

7. A natural number n is *perfect* just when the sum of all the positive divisors of n is $2n$.
   (i) (Euclid) Suppose that $2^q - 1$ is prime. Show that $n = 2^{q-1}(2^q - 1)$ is a perfect number.
   (ii) (Euler) Prove that if an even natural number is perfect then it is of the form $n = 2^{q-1}(2^q - 1)$, where $2^q - 1$ is prime.

   (It is conjectured that there are no odd perfect numbers but this is not known.)

8. (i) Find the smallest non-negative integer x satisfying the congruences $x \equiv 2 (\mathrm{mod}\, 3)$, $x \equiv 3 (\mathrm{mod}\, 5)$, $x \equiv 4 (\mathrm{mod}\, 11)$, $x \equiv 5 (\mathrm{mod}\, 16)$.
   (ii) Find all integers x satisfying both $19x \equiv 103 (\mathrm{mod}\, 900)$ and $10x \equiv 511 (\mathrm{mod}\, 841)$.

9. A positive integer is said to be *square-free* if it is the product of distinct primes. (So 174 is square-free but 175 is not, for example.) Are there 100 consecutive numbers that are *not* square-free?

10. Prove that the classes of both 2 and 3 generate $(\mathbb{Z}/5^n\mathbb{Z})^\times$ for all positive integers n. For each of the primes $p = 11$, 13, 17 and 19, find a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for all $n \geqslant 1$.

11. Let A be the group $(\mathbb{Z}/65520\mathbb{Z})^\times$. Determine the least positive integer n such that $g^n = 1$ for all g in A.

12. Let a and n be integers greater than 1, and put $N = a^n - 1$. Show that the order of $a + N\mathbb{Z}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ is exactly n, and deduce that n divides $\phi(N)$. If n is a prime, deduce that there are infinitely many primes q such that $q \equiv 1 (\mathrm{mod}\, n)$.

That ends the official part of the sheet. The remaining questions are intended to encourage investigation so don't bother your supervisor with them.

(A) Think about linear Diophantine equations of the form $ax + by = c$, where a, b and c are fixed natural numbers. We are interested in integer solutions (x, y). Try to develop some theory. In particular is it possible for such an equation to have (i) no solutions, (ii) exactly one solution, (iii) infinitely many solutions? If so when?

(B) This refers to question 2 above. Let a and b be four-digit numbers. What is the least value which $\lambda(a, b)$ can take? Find a and b so that $\lambda(a, b)$ is fairly large. How do you do relative to the bound given in the question? Can you see what the worst case will be?

(C) We show in lectures that for p an odd prime, the multiplicative group of units mod p^n is cyclic. Can you determine the structure of the multiplicative group of units mod 2^n?

Email any comments, suggestions and queries to `m.hyland@dpmms.cam.ac.uk`.