Number theory: Problem sheet 4

Solutions to indicated questions and parts of questions must be submitted by Friday 10 January 2014
You are encouraged to submit solutions to non-assessed problems too

Some of the computational examples ask you to use `MAPLE`. This package is somewhat similar to `MATLAB`. In computational number theory it is essential one uses a system that can deal with integers of arbitrary length; `MAPLE` does but as far as I am aware `MATLAB` doesn't. If you are really keen on programming you could use a language like `Python` instead (which supports arbitrary length integers) but then you would need to write your own version of the Euclidean algorithm etc. There are lots of introductions to `MAPLE` online. One convenient one is at
`www.personal.soton.ac.uk/jav/soton/maple/Maple11Tutorial.pdf` .
The good thing is that one does not need very much `MAPLE` for our examples. Most of what you need is illustrated in the handouts on "the extended Euclidean algorithm", "the binary powering algorithm" and "algorithms in `MAPLE`" on the webpage. Some other useful commands: `isprime` detects if an integer is prime and `ifactor` factorizes it into primes.

1. (B) A *perfect number* is a natural number n whose positive divisors (excluding n itself) add up to n. Thus, for example, 28 is a perfect number since $1+2+4+7+14 = 28$. Prove that $2^{k-1}(2^k - 1)$ is perfect whenever $2^k - 1$ is prime. Also, find all perfect numbers of this form with $k \leq 30$. (You are advised to use `MAPLE` to check whether $2^k - 1$ is prime.)

   [Euler proved that every even perfect number has the form described above. It is still unknown whether there are any odd perfect numbers.]

2. (A) Apply Pollard's $p - 1$ algorithm, showing your working, with base $a = 2$ to find a prime factor of $n = 6527$. [10 marks]

3. (A) Apply Pollard's Rho algorithm, by hand, with iteration function $f(x) = x^2 + 1$ and seed $x_0 = 2$ to find a prime factor of $n = 4847$. How many iterations did you need? [15 marks]

4. (A) Using the `MAPLE` implementation of Pollard Rho from the website (or if you prefer you can rewrite it in your favourite computer language or computer algebra system), find prime factors of each of the following numbers n, using seed $x_0 = 2$ and iteration function $f(x) = x^2 + 1$.

   (i) $2^{47} - 1$; (ii) $2^{71} - 1$; (iii) $10^{21} - 3$.

   In each case, give the number of iterations needed. (You will need to modify the given code to output the number k as well as g.) [(iii): 15 marks]

5. (A) Apply the Fermat test, by hand, to each of the following numbers n with base a:

   (i) $n = 257$, $a = 3$; (ii) $n = 1201$, $a = 2$; (iii) $n = 1729$, $a = 2$.

   In each case, what do you conclude?

6. (B) An early triumph of the Pollard Rho method was the factorization of $2^{256} + 1$, already known to be composite, by Brent and Pollard in 1980. They wrote up their proof in the paper 'Factorization of the eighth Fermat number', which was published in 1981 in the journal *Mathematics of Computation*, volume 36, pages 627–630.

   Download this paper from the JSTOR archive: `http://www.jstor.org/` (you may need to be on campus to do this). Which iteration function did they use to factorize $2^{256} + 1$? What seed did they use? How long did their calculation take? What is their mnemonic for the factor?

   (If you are feeling energetic, repeat their calculation in `MAPLE`.)

7. (B) Let p be a prime, and let q be a prime factor of $2^p - 1$. Prove that $\mathrm{ord}_q(2) = p$, and deduce that $q \equiv 1 \pmod{p}$. [15 marks]

   Hence show, by hand, that $2^{13} - 1$ and $2^{17} - 1$ are both prime, and find prime factors of each of $2^{23} - 1$ and $2^{29} - 1$ (you should show your working). [15 marks]

8. (B) Let p be prime, and let a be a positive integer with $p \nmid (a - 1)$. Let $m = (a^p - 1)/(a - 1)$, which is an integer, and let q be a prime factor of m. Prove first that $p \nmid m$ and so that $q \neq p$. Then prove that a has order p modulo q, and deduce that $q \equiv 1 \pmod{p}$.

   By choosing $a = n!$, or otherwise, deduce that there are infinitely many primes q satisfying $q \equiv 1 \pmod{p}$.

9. (B) Let p be a prime with $p \equiv 1 \pmod{3}$. Prove that there is an integer a such that $\mathrm{ord}_p(a) = 3$. Let $b = a - a^2$. Prove that $b^2 \equiv -3 \pmod{p}$, and deduce, without appealing to Gauss's lemma or quadratic reciprocity, that $\left(\frac{-3}{p}\right) = 1$. [15 marks]

10. (A) Compute the Legendre symbol $\left(\frac{5}{p}\right)$ from scratch using Gauss's lemma (as I did for $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$ in lectures).

11. (B) Prove that for each odd positive integer n the Jacobi symbol satisfies

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 1 \pmod{4} \end{cases}$$

and

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

(You may assume thse hold for the Legendre symbol).

12. (A) Find all quadratic residues modulo 29. [5 marks]

13. (A) Evaluate (showing your working) the following Legendre symbols:

(i) $\left(\frac{77}{97}\right)$; (ii) $\left(\frac{133}{211}\right)$; (iii) $\left(\frac{1066}{2011}\right)$. [(iii): 5 marks]

Make up some examples of your own, and compute them until you are completely comfortable with the process.

14. (B) Prove that the congruence

$$x^8 \equiv 16 \pmod{p}$$

is soluble for **every** prime p.

15. (A) In each case, the prime p is congruent to 3 modulo 4. By computing $a^{(p+1)/4}$ (using `MAPLE` if necessary) solve the congruence $x^2 \equiv a \pmod{p}$.

(i) $p = 103$, $a = 7$; (ii) $p = 211$, $a = 11$;
(iii) $p = 2011$, $a = 666$. [(iii): 5 marks]

16. (B) For each odd prime p define $p^* = \left(\frac{-1}{p}\right)p$. Prove that $p^* \equiv 1 \pmod{4}$. Also prove that the Law of Quadratic Reciprocity is equivalent to the statement that

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

for all odd primes p and q.

17. (C) Let p be an odd prime number. Define

$$\tau_p = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \exp(2\pi i a/p).$$

Prove that $\tau_p^2 = \left(\frac{-1}{p}\right)p$. (Much harder!) Determine the value of τ_p.

RJC 21/11/2013