Number Theory Example Sheet 1
Michaelmas 2004

Dr Alessio Corti

14 October, 2004

(1) Calculate the greatest common divisor $d = (a, b)$ and find integers (x, y) such that $ax + by = d$ in the following cases:

$$(i)\ a = 841, b = 160 \quad (ii)\ a = 2613, b = 2171 \quad (iii)\ a = 8991, b = 3293$$

(2) Let a, b be positive integers with $a > b > 1$. Let $\lambda(a, b)$ be the number of steps (i.e. individual applications of the Euclidean algorithm) required to compute $d = (a, b)$ via successive applications of the Euclidean algorithm. Clearly $\lambda(a, b) < b$. Prove that

$$\lambda(a, b) \leq 2\frac{\log b}{\log 2}$$

(3) (i) Suppose that n is known to be the product of two primes. Show how one can determine these primes from the knowledge of n and $\varphi(n)$.

(ii) Suppose that n is not a perfect square, and satisfies

$$n - n^{2/3} < \varphi(n) < n - 1.$$

Deduce that n is the product of two distinct primes.

(4) Let p be a prime dividing $b^n - 1$, where b and n are integers > 1. Show that either $p \equiv 1 \mod n$, or $p | b^d - 1$ for some divisor d of n. If $p > 2$ and n is odd, then in the second case $p \equiv 1 \mod 2n$. Using this, find the prime factorization of the following numbers:

$$2^{11} - 1 = 2047, \quad 3^{12} - 1 = 531440, \quad 2^{35} - 1 = 34359738367.$$

[Hint: If $p | 2^{11} - 1$, for example, then $p \equiv 1 \mod 22$ so test $p = 23, 67....$ You only need to test up to $\sqrt{2047}$.]

(5) (i) Find the smallest nonnegative integer x such that

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 11 \\ x \equiv 5 \mod 16 \end{cases}$$

(ii) Find the smallest nonnegative integer x satisfying

$$\begin{cases} 19x \equiv 103 \mod 900 \\ 10x \equiv 511 \mod 841 \end{cases}$$

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

(7) Prove that -2 is a primitive root modulo 23. Determine all solutions to the congruences $x^7 = 17 \mod 23$ and $x^{26} \equiv 10 \mod 23$.

(8) Find a generator of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ for $p = 5, 7, 11, 13$. Determine how many of the integers $1, 2, ..., p-1$ are generators.

(9) Suppose that $p | 2^{2^k} + 1$, where $k > 1$. Then:

1. Show that $p \equiv 1 \mod 2^{k+1}$.
2. By asking whether 2 is a quadratic residue $\mod p$, show that $p \equiv 1 \mod 2^{k+2}$.
3. Use this to show that $2^{16} + 1$ is prime.