Homework 2 (due Monday, Dec. 3)

Correct solutions to any 8 problems gives 5 bonus points on the exam. All your work must be properly motivated !

Q.1. Find all primitive roots modulo 29.

Q.2 Compute the Legendre-Jacobi symbol

$$\left(\frac{16144}{377}\right).$$

Q.3 As in the lectures, let S_2 denote the set of positive integers which can be expressed as the sum of two integer squares. Prove that the upper asymptotic density of the set S_2 is zero.

Q.4 Suppose the natural number n is a product of two distinct primes p and q. Assuming both n and $\phi(n)$ are known, show how one would find p and q as efficiently as possible.

(HINT: The point is you can write down an explicit formula for p and q in terms of the known quantities).

Q.5 Let notation be as in Exercise 7 on Homework 1.

(i) Let $\mathcal{L}$ be an invariant linear equation, i.e.: $\sum_{i=1}^{n} a_i = a_0 = 0$. Assume the following property (*) holds :

(*) For any subset A of $\mathbb{Z}$ not containing any non-trivial solutions to $\mathcal{L}$, one has $\overline{d}(A) = 0$.

Deduce that the limit $\lim_{n\to\infty} f(n)/n = 0$.

(ii) There is a famous theorem of Szemerédi from 1975 which states that any subset of $\mathbb{Z}$ of strictly positive upper asymptotic density must contain arbitrarily long arithmetic progressions (this extends Roth's theorem). Assuming this result, deduce that property (*) does indeed hold for any invariant linear equation.

(REMARK : I haven't given a precise definition of what is meant by a 'trivial solution', but you can consider it part of this exercise to give such a precise definition. Informally, trivial solutions are those which any non-empty set cannot avoid having).

Q.6 (i) Let $a, b, c, d \in \mathbb{Z}$. Give necessary and sufficient conditions for the vectors $\vec{e}_1 = (a, b)$ and $\vec{e}_2 = (c, d)$ to generate the integer lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$.

(ii) More generally, let $n \in \mathbb{N}$ and let $\{v_1, ..., v_n\}$ and $\{w_1, ..., w_n\}$ be two bases for $\mathbb{R}^n$, as a vector space over $\mathbb{R}$. Describe necessary and sufficient conditions for these two sets of vectors to generate the same lattice in $\mathbb{R}^n$.

Q.7 Explain why the condition of boundedness is not necessary in Minkowski's theorem. On the other hand, give examples which illustrate how the theorem may fail if either of the conditions of symmetry or convexity is dropped, even if the set remains connected.

Q.8 Prove that, as $N \to \infty$,

$$\sum_{n=1}^{N} d(n) \sim N \log N \quad \text{and} \quad \sum_{n=1}^{N} \sigma(n) \sim \frac{\pi^2}{12} N^2.$$

Q.9 Determine infinite series representations for each of the following functions, in terms of the various multiplicative functions discussed in Week 46. Indicate in what range of $s \in \mathbb{C}$ each representation is valid :

$$\textbf{i}.\ \frac{\zeta(s-1)}{\zeta(s)} \quad \textbf{ii}.\ (\zeta(s))^2 \quad \textbf{iii}.\ \zeta(s)\zeta(s-1).$$

Q.10 Let p be a prime. Prove that the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p, where μ is the Möbius function.

Q.11 Let p be a prime greater than 3. Prove that the numerator in the fraction

$$\sum_{k=1}^{p-1} \frac{1}{k},$$

when written in lowest terms, is divisible by p^2.