Homework 2 (due Wednesday, Dec. 12)

There is a total of 33 points available, and maximum points yield 6 bonus points on the exam. Thus, if you score $x/33$ you will be awarded $6x/33$ bonus points. All your work must be properly motivated !

Q.1 (3p) Give a rigorous proof of the following statement: For $n \in \mathbb{N}$, let p_n be the probability that GCD$(a, b) = 1$, when the numbers a and b are chosen independently and uniformly at random from $\{1, 2, \ldots, n\}$. Then $p_n \to \frac{6}{\pi^2}$ as $n \to \infty$.

Q.2 (1p) Explain why one has the condition that a not be a perfect square in Artin's conjecture.

Q.3 (2p) Find all primitive roots modulo 37.

Q.4 (3p+1p) For $n \in \{2, 3\}$, let S_n denote the set of positive integers which can be expressed as the sum of (at most) n integer squares. Prove that $\overline{d(S_2)} = 0$ and compute $d(S_3)$.

Q.5 (5x1p) Let p be a prime congruent to $1 \pmod 4$. Let

$$S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}.$$

(i) Show that the set S is non-empty.
(ii) Show that, if $(x, y, z) \in S$, then $x \neq y - z$ and $x \neq 2y$.

Let $f : S \to S$ be the map given by

$$f(x,y,z) = \begin{cases} (x + 2z,\, z,\, y - x - z), & \text{if } x < y - z, \\ (2y - x,\, y,\, x - y + z), & \text{if } y - z < x < 2y, \\ (x - 2y,\, x - y + z,\, y), & \text{if } x > 2y. \end{cases}$$

(iii) Show that f is well-defined, i.e.: that it is defined on all of S and that $f(S) \subseteq S$.
(iv) Show that f is one-to-one on S and has a unique fixed point. Determine also the latter.
(v) By considering the map $g : S \to S$ given by $g(x, y, z) = (x, z, y)$, deduce that p is a sum of two squares.

Q.6 (2p) Compute the Legendre-Jacobi symbol

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

Q.7 (2p+2p) Let notation be as in Exercise 5 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.8 (2p+2p) 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 (1p+1p+1p) Determine infinite series representations for each of the following functions, in terms of the various multiplicative functions discussed in the lecture notes. 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 (2p) 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 (3p) 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.