Math 453 - December 20, 2013
Final exam

The first five problems are mandatory. Solve ONLY five of problems 6-10. Each problem is worth 10 points. Perfect score = 100 pts.

Part I. Solve all problems 1-5 below.

[1] (i) (5 pts.) Prove that if $m, n \in \mathbb{N}$ and $m|n$, then $(5^m - 1)|(5^n - 1)$.
(ii) (3 pts.) Prove that if $a, b \in \mathbb{N}$, then $(a, b) = 1$ if and only if $(a + b, ab) = 1$.
(iii) (2 pts.) Is it true in general that $(a, b) = (a + b, ab)$ for every $a, b \in \mathbb{N}$? Provide a proof or counterexample.

[2] Find:
(i) (3 pts.) A multiplicative inverse modulo $m = 47$ of $n = 30$.
(ii) (3 pts.) A particular solution $(x, y) \in \mathbb{Z}^2$ of the equation

$$30x + 47y = 1.$$

(iii) (2 pts.) All solutions $(x, y) \in \mathbb{Z}^2$ of the equation in (ii).
(iv) (2 pts.) The least nonnegative solution of the system $\begin{cases} x \equiv 3 \pmod{12} \\ x \equiv 6 \pmod{19}. \end{cases}$

[3] (i) (5 pts.) Prove that $\varphi(n) = n \displaystyle\sum_{d|n,\, d>0} \frac{\mu(d)}{d}$.
(ii) (5 pts.) Prove that $\displaystyle\sum_{1\le n\le X} \mu(n) \left[\frac{X}{n}\right] = 1$ for all $X \ge 1$ (X not necessarily integer).
Here $[a]$ denotes the integer part of $a \in \mathbb{R}$.

[4] (i) (5 pts.) Evaluate the Legendre symbol $\left(\dfrac{31}{641}\right)$.
(ii) (5 pts.) If p is an odd prime number not equal to 5, evaluate $\left(\dfrac{-5}{p}\right)$.

[5] (i) (3 pts.) Show that if $d \ge 2$ is an integer, then

$$\sqrt{d^2 + 2} = [d; \overline{d, 2d}].$$

(ii) (2 pts.) Compute the convergents C_0, C_1, C_2, C_3 of $\sqrt{11}$.
(iii) (3 pts.) What are the inequalities satisfied by $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and its convergents $C_{2k} = \frac{p_{2k}}{q_{2k}}$ and $C_{2k+1} = \frac{p_{2k+1}}{q_{2k+1}}$? Use them to prove that

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

(iv) (2 pts.) What is a quadratic irrational number? What is known about the simple continued fraction expansion of a quadratic irrational?

Solve five out of the next six problems.

[6] (i) (5 pts.) Find the last two digits of the decimal expansion of 2^{2013}.
(ii) (5 pts.) Show that if p is an odd prime, then

$$2\,(p - 3)! \equiv -1 \pmod{p}.$$

[7] (i) (5 pts.) Find all values of $n \in \mathbb{N}$ for which $\varphi(5n) = 4\varphi(n)$.

(ii) (5 pts.) Show that if p is a prime number and $a \in \mathbb{Z}$ with $p \nmid a$, then

$$(a+p)^{p-1} \not\equiv a^{p-1} \pmod{p^2}.$$

[8] (i) (5 pts.) Let $s > 1$. Show that the series $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ is absolutely convergent and find the Euler product expression for $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)^2}{n^s}$. Justify your calculations.

(ii) (5 pts.) Prove the equality

$$\sum_{n=1}^{\infty} \frac{\mu(n)^2}{n^s} = \frac{\zeta(s)}{\zeta(2s)} \quad \text{if } s > 1.$$

[Recall that $\displaystyle\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ and $\displaystyle\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ if $s > 1$.]

[9] (i) (3 pts.) Show that if $a'a \equiv 1 \pmod{m}$, then $\text{ord}_m(a) = \text{ord}_m(a')$.

(ii) (3 pts.) Knowing that 17 is a primitive root modulo 311, find $\text{ord}_{311}(17^{10})$.

(iii) (4 pts.) Decide whether it is true that if m is a positive integer and d is a divisor of $\varphi(m)$, then there exists an integer a with $\text{ord}_m(a) = d$. Give reasons for your answer.

[10] (i) (2 pts.) How many primitive roots modulo 29 are there?

(ii) (4 pts.) Find a primitive root r modulo 29.

(iii) (4 pts.) Use index arithmetic to find all solutions of the congruence

$$3x^{18} \equiv 4 \pmod{29}.$$

[11] (i) (6 pts.) Prove that rational numbers do not admit infinite simple continued fraction expansions.

(ii) (4 pts.) Let $\beta \in (0,1) \setminus \mathbb{Q}$ with convergents $\frac{p_n}{q_n}$. Show that, for all $n \in \mathbb{N}$,

$$|q_{n+1}\beta - p_{n+1}| < |q_n\beta - p_n|.$$