Math 453 - December 17, 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) (6 pts.) Prove that if $2^n - 1$ is a prime number for some $n \in \mathbb{N}$, then n is a prime number.

(ii) (4 pts.) Prove that if $a, b \in \mathbb{N}$, then

$$(a, b) = (a + b, [a, b]).$$

[2] Find:

(i) (3 pts.) A multiplicative inverse modulo $m = 81$ of $n = 40$.

(ii) (3 pts.) A particular solution $(x, y) \in \mathbb{Z}^2$ of the equation

$$40x + 81y = 1.$$

(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 $\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17}. \end{cases}$

[3] (i) (5 pts.) State the Möbius Inversion Theorem.

(ii) (5 pts.) Prove that $\varphi(n) = n \sum_{d|n,\, d>0} \frac{\mu(d)}{d}$.

[4] (i) (5 pts.) State the Quadratic Reciprocity Law.

(ii) (5 pts.) For which values of the prime number p is the congruence $x^2 + 3 \equiv 0 \pmod{p}$ solvable in $\mathbb{Z}$?

[5] (i) (3 pts.) Find the irrational number α with simple continued fraction expansion

$$\alpha = [9; \overline{1, 18}\,].$$

(ii) (2 pts.) Compute the convergents C_0, C_1, C_2, C_3 of α.

(iii) (3 pts.) What are the inequalities satisfied by α, C_{2k} and C_{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 do you know about the simple continued fraction expansion of $\sqrt{n}$ when $n \in \mathbb{N}$ is not a perfect square?

Solve five out of the next six problems.

[6] (i) (5 pts.) Find the last digit of the decimal expansion of 3^{1000}.

(ii) (5 pts.) Prove that if p is an odd prime, then

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

[7] (i) (5 pts.) Show that if m and n are positive integers with $m|n$, then $\varphi(m)|\varphi(n)$.

(ii) (5 pts.) Show that if p is a prime number and $a, h \in \mathbb{Z}$ are such that $(a + h)^p \equiv a^p \pmod{p}$, then $(a + h)^p \equiv a^p \pmod{p^2}$.

[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 $\displaystyle\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s}$. Justify your calculations.

(ii) (5 pts.) Prove the equality

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

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

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

(ii) (3 pts.) Knowing that 6 is a primitive root modulo 251, find $\mathrm{ord}_{251}(6^{25})$.

(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 $\mathrm{ord}_m(a) = d$. Give reasons for your answer.

[10] (i) (2 pts.) How many primitive roots modulo 23 are there?

(ii) (4 pts.) Find a primitive root r modulo 23.

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

$$3x^{14} \equiv 2 \pmod{23}.$$

[11] Let α be an irrational number. Show that:

(i) (6 pts.) For any two consecutive convergents $C_n = \frac{p_n}{q_n}$ and $C_{n+1} = \frac{p_{n+1}}{q_{n+1}}$ of α, there exists $i \in \{n, n+1\}$ such that

$$\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{2q_i^2}.$$

Hint: You can use the first part of (iii) in Problem 5.

(ii) (4 pts.) If $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $(a, b) = 1$ and

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is a convergent of α.

Hint: You can use the equivalence $\frac{a}{b}$ convergent for $\alpha \iff \frac{a}{b}$ best approximation of α.