Instructor: Leo Goldmakher

NAME: ________________________________

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 8 – due Thursday, November 29th

INSTRUCTIONS:

This assignment should be turned in to me in person (i.e. don't leave them in my mailbox or ask someone else to submit on your behalf) at the beginning of Thursday's class. Late assignments may be left in my mailbox (just inside the entrance to Bascom) by **4pm** on Friday; however, 5% will be deducted for late submission. *Assignments submitted later than 4pm on Friday will not be graded.*

Please print and attach this page as the first page of your submitted problem set.

PROBLEM	**GRADE**
8.1	
8.2	
8.3	
8.4	
Total	

Please read the following statement and sign **before starting this problem set:**

I understand that I am not allowed to use the internet to assist with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person, and to not copy from any set of written notes created when another person was present. I pledge to abide by the Williams honor code.

SIGNATURE:________________________________

Problem Set 8

8.1 In the last problem set you explored a method for efficiently extracting square-roots (mod p); this is called the *Tonelli-Shanks algorithm.* In class (Lecture 18) we saw how to combine this with the Chinese Remainder Theorem to efficiently solve congruences of the form

$$(*) \qquad x^2 \equiv a \pmod{pq},$$

but our method only worked if we know p and q. The goal of this exercise is to prove the converse: that if there exists an algorithm that efficiently extracts square-roots (mod pq), then we can efficiently factor pq. Thus, extracting square-roots (mod pq) is equivalently hard to factoring pq.

Fix distinct odd primes p and q, write $\overline{p} := \frac{1}{p} \pmod{q}$ and $\overline{q} := \frac{1}{q} \pmod{p}$, and set

$$\mu := p\overline{p} - q\overline{q} \pmod{pq}.$$

(a) Prove that $\mu^2 \equiv 1 \pmod{pq}$.

(b) Prove that $\mu \not\equiv \pm 1 \pmod{pq}$.

(c) Prove that $(\mu + 1, pq) = p$.

(d) Suppose there exists an efficient algorithm for taking square-roots (mod pq), i.e. some algorithm that, given any a, produces all solutions to $(*)$. Describe an efficient algorithm for finding the prime factorization of pq.

(e) Prove that if $\alpha \in \mathbb{Z}_{pq}$ is a solution to the congruence $(*)$, then $\{\pm\alpha, \pm\mu\alpha\}$ is a complete set of solutions (mod pq).

(f) Suppose there exists an efficient algorithm that produces *one* particular choice of $a \in \mathbb{Z}_{pq}^{\times}$ and four solutions to $(*)$ for this a. (Compare this to (d), in which the algorithm is assumed to work for *every* choice of a.) Describe an efficient algorithm for finding the prime factorization of pq.

8.2 The goal of this problem is to develop a different (and ingenious!) approach to Fermat's two-squares theorem; it was apparently first discovered by Thue in the early 20th century. Fix a prime $p \equiv 1 \pmod 4$.

(a) Prove the existence of $\gamma \in \mathbb{Z}$ such that $\gamma^2 \equiv -1 \pmod{p}$.

- **For the rest of the problem, fix a suitable choice of γ from part (a).**

(b) Suppose there exist integers a, b, not both zero, such that

$$|a| \le \sqrt{p} \quad , \quad |b| \le \sqrt{p} \quad , \quad \text{and} \quad a \equiv b\gamma \pmod{p}.$$

Prove that $p = a^2 + b^2$.

(c) Let $k := \lfloor \sqrt{p} \rfloor$, and suppose $f : \mathbb{Z}_{k+1} \times \mathbb{Z}_{k+1} \longrightarrow \mathbb{Z}_p$ is a function. Prove that f cannot be an injection.

(d) Consider the function defined by $f(m, n) := m - n\gamma \pmod{p}$. Use the previous parts of this problem to deduce that p is the sum of two squares.

8.3 Some problems about $\mathbb{C}$. If $z := a + bi$ with $a, b \in \mathbb{R}$, we say that a is the *real part of* z, denoted $\text{Re } z := a$, and b is the *imaginary part of* z, denoted $\text{Im } z := b$.

(a) Let $\mathbb{Q}[i] := \{z : \text{Re } z, \text{Im } z \in \mathbb{Q}\}$. Prove that for any $\alpha, \beta \in \mathbb{Q}[i]$ we have $\overline{\alpha}, \alpha + \beta, \alpha\beta, \frac{\alpha}{\beta} \in \mathbb{Q}[i]$. (In the last of these, assume that $\beta \neq 0$.)

(b) Give an example of $\alpha \in \mathbb{Q}[i]$ such that $|\alpha| \notin \mathbb{Q}[i]$.

(c) For any $z \in \mathbb{C}$, prove that $\text{Re } z = \frac{1}{2}(z + \overline{z})$ and $\text{Im } z = \frac{1}{2i}(z - \overline{z})$.

(d) Prove that $\overline{zw} = \overline{z}\,\overline{w}$ and $\overline{z + w} = \overline{z} + \overline{w}$ for all $z, w \in \mathbb{C}$.

(e) Recall the following Taylor series expansions:

$$\begin{aligned}\sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots \\ \cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots \\ e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \cdots\end{aligned}$$

Show that $e^{i\theta} = \cos\theta + i\sin\theta$. (You don't have to worry about convergence of infinite series.)

(f) Use part (e) to find formulas for $\sin 3\theta$ and $\cos 3\theta$. (This shouldn't take much work!)

(g) Let $e(x) := e^{2\pi i x}$. On the complex plane, draw (and label) the points $e(1/4)$, $e(1/2)$, $e(-1/4)$, and $e(2/3)$.

(h) Given any $k \in \mathbb{Z}$. Evaluate $\displaystyle\int_0^1 e(kx)\,dx$. [*The answer is nice, but use caution!*]

(i) Let $r_4(k)$ denote the number of ways of writing k as the sum of four squares, i.e.

$$r_4(k) := \#\{(a,b,c,d) \in \mathbb{Z}^4 : k = a^2 + b^2 + c^2 + d^2\}$$

Prove that

$$r_4(k) = \int_0^1 \Theta(x)^4 \, e(-kx)\,dx,$$

where $\Theta(z) := \sum_{n\in\mathbb{Z}} e(n^2 z)$. [*Don't worry about details of whether or not things converge!*]

8.4 Recall that $\alpha \in \mathbb{Z}[i]$ is a *unit* iff $|\alpha| = 1$.

(a) Prove that the only units of $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.

(b) If two nonzero elements of $\mathbb{Z}$ have the same magnitude, then their ratio must be a unit. Does this also hold in $\mathbb{Z}[i]$? Either prove it or give a counterexample.

(c) Let $\alpha := 27 - 23i$ and $\beta := 8 + i$. Find $\kappa, \rho \in \mathbb{Z}[i]$ such that $\alpha = \kappa\beta + \rho$ and $0 \leq |\rho| < |\beta|$. (*Note that ρ is the Greek letter* rho, *not the Latin letter p.*)

(d) Prove that the quotient-remainder theorem holds in $\mathbb{Z}[i]$: given any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, prove that there exist $\kappa, \rho \in \mathbb{Z}[i]$ such that $\alpha = \kappa\beta + \rho$ and $0 \leq |\rho| < |\beta|$.

(e) Show by example that the choices of κ and ρ in the quotient-remainder theorem for $\mathbb{Z}[i]$ are *not* unique!