MATH 4400/6400 – Homework #2

posted January 30, 2019; due Feb. 6, 2019

The mathematician Pascal admires the beauty of a theorem in number theory; it's as though he were admiring a beautiful natural phenomenon. It's marvellous, he says, what wonderful properties numbers have. It's as though he were admiring the regularities in a kind of crystal. — L. Wittgenstein

Directions. Give complete solutions, providing full justifications when appropriate. Your assignment must be stapled if it goes on beyond one page. Starred problems are required for MATH 6400 students and extra credit for 4400 students.

1. Show that if a, b, and c are positive integers, then $\gcd(ac, bc) = c \cdot \gcd(a, b)$.

2. Compute 2^{90} mod 91 and 3^{90} mod 91; show your work! By "compute mod 91", I am asking for the least nonzero remainder when you divide by 91.

   Hint: To compute 2^{90}, compute each of $2, 2^2, 2^4, 2^{16}, 2^{32}, 2^{64}$ mod 91, and then multiply an appropriate combination of them to get 2^{90}. Do something similar for 3^{90}.

3. Show that if $x \in U(\mathbf{Z}_{1105})$, then $x^{1104} = [1]$. **WARNING:** 1105 is not a prime number!

4. Let p be a prime number, with $p \equiv 1 \pmod 3$.

   (a) Explain how you know that $U(\mathbf{Z}_p)$ contains an element of order 3. (You may assume that $U(\mathbf{Z}_p)$ is cyclic, as we will show in class.)

   (b) Show that there is an element of $\mathbf{Z}_p$ which squares to $[-3]$.

   For example, if $p = 19$, then $[4]^2 = [-3]$.

   Hint for (b): Show that if $u \in U(\mathbf{Z}_p)$ has order 3, then u is a root of $x^2 + x + 1 \in \mathbf{Z}_p[x]$. Then "complete the square."

5. Let p be an odd prime. Prove that

$$(1+p)^p \equiv 1 \pmod{p^2}.$$

   More generally, show that for each integer $k \geq 1$,

$$(1+p)^{p^k} \equiv 1 \pmod{p^{k+1}}, \quad \text{but} \quad (1+p)^{p^k} \not\equiv 1 \pmod{p^{k+2}}.$$

6. Let G, H be abelian groups. A *homomorphism* $\phi\colon G \to H$ is a map from G to H with the property that

$$\phi(gg') = \phi(g)\phi(g') \qquad \text{for all } g, g' \in G,$$

   where the left-hand 'multiplication' gg' takes place in G and the right-hand 'multiplication' $\phi(g)\phi(g')$ takes place in H. We say ϕ is an *isomorphism* if ϕ is a homomorphism and also a bijection. We write $G \cong H$ if there is an isomorphism from G to H.

   Just as in MATH 4000, 'isomorphism' should be thought of as 'being the same up to relabeling'. In particular, isomorphism is an equivalence relation on the class of groups, and two groups that are isomorphic share any property that can be expressed in the language of groups.

   (a) Classify all cyclic groups by showing that if G is a cyclic group, then G is isomorphic to either (a) $\mathbf{Z}$ (under addition) or (b) $\mathbf{Z}_m$ (under addition) for some $m \in \mathbf{Z}^+$.

   (b) Show that $\mathbf{Q}$ under addition is not isomorphic to $\mathbf{Z}$ under addition.

7. (a) Show that if R and S are commutative rings, and $R \cong S$ as rings, then $U(R) \cong U(S)$ as abelian groups. *Hint:* Check that your ring isomorphism restricts to a group isomorphism.

(b) In MATH 4000, you proved that if m and n are relatively prime positive integers, then $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$. Use this and the result of (a) to conclude that $\phi(mn) = \phi(m) \cdot \phi(n)$. Thus, ϕ is what we have been calling a *multiplicative* function.

8. Generalize the result of Problem 3 to show that if the positive integer n has the prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, and L is any common multiple of $\phi(p_1^{e_1}), \dots, \phi(p_k^{e_k})$, then $x^L = 1$ for all $x \in U(\mathbf{Z}_n)$. Use this to prove that if n is divisible by at least two different odd primes, then $U(\mathbf{Z}_n)$ is not cyclic.

9. Define a complex-valued function μ on the positive integers by declaring that $\mu(1) = 1$ and requiring that
$$\sum_{d|n} \mu(d) = 0 \qquad \text{for all integers } n > 1.$$
Show that these conditions uniquely determine μ. Compute $\mu(n)$ for all $n \leq 20$. Any conjectures?

10. Define the *Farey sequence* $\mathfrak{F}_n$ of order n as the list of reduced fractions in $[0,1]$ with denominator not exceeding n, arranged in increasing order. For example, $\mathfrak{F}_1 = \{\frac{0}{1}, \frac{1}{1}\}$, and $\mathfrak{F}_4 = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$.

    Compute $\mathfrak{F}_n$ for all $n = 1, 2, 3, 4, 5, 6, 7$. Formulate a conjecture about differences of consecutive Farey fractions.

11. (*) Prove that 6 is the only squarefree perfect number.

    Here a *squarefree* number is a positive integer that can be written as a product of distinct primes. For example, $35 = 5 \cdot 7$ is squarefree, but $36 = 2^2 \cdot 4$ is not. Recall also that a *perfect number* is a positive integer N for which $\sum_{d|N} d = 2N$.