

4400/6400 PROBLEM SET 6

Recommendations: 4400 students should solve at least five of the problems; 6400 students should solve at least seven.

6.1: If $m|n$ are positive integers, show that $\varphi(m) \mid \varphi(n)$.

6.2: Let G be a cyclic group of order n and x an element of G of order d . Let e be a positive integer. Show that the order of x^e is $\frac{d}{\gcd(d,e)}$.
(Feel free to take G to be the additive group Z_n of the integers modulo n and x to be some residue class $k \pmod{n}$. This shows that it is really a number theory problem after all.)

6.3: Let G be a cyclic group of *even* order $2k$.

- a) Show that G has a unique element, say t , of order 2.
- b) Show that for any $x \in G$, x^k is either equal to the identity element 1 of G or to the element t of order 2.
- c) Show that $x^k = 1$ iff there exists $y \in G$ such that $x = y^2$. (Use Problem 6.2).
- d) Recalling that for an odd prime p , $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, deduce Euler's criterion: for $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, there exists a such that $x \equiv a^2 \pmod{p}$ iff $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

6.4: a) Use 6.3d) with $x = -1$ to show that an odd prime p divides $a^2 + 1$ for some integer a iff $p \equiv 1 \pmod{4}$.¹

b) Use Euler's criterion to check, for each odd prime $p \leq 50$, whether 2 is a quadratic residue modulo p . Can you find a pattern?

6.5: a) Show that the function

$$g(n) = \frac{n}{e^\gamma \log \log n + \frac{3}{\log \log n}}$$

is monotonically increasing.²

b) Use the fact that $\varphi(n) \geq g(n)$ for all $n \geq 3$ to find all n for which $\varphi(n) = 100$. (Tip: $e^\gamma \approx 1.781$.)

6.6: We proved in class that for every $\epsilon > 0$, there exists an n with $\varphi(n) < \epsilon n$.

- a) Find an n such that $\varphi(n) < \frac{1}{5}n$.
- b)* Can you find an explicit value of n such that $\varphi(n) < \frac{1}{10}n$? (You will almost certainly want some computer help with this.)

6.7: a) Show that for any $\delta > 0$, $\lim_{n \rightarrow \infty} \frac{d(n)}{n^\delta} = 0$. (Hint: $d(n)/n^\delta$ is multiplicative,

¹This was also explained in class, but it is very important, and I'd like you to look it over again to make sure.

²Of course, it suffices to show that its derivative is positive. . .

so applying Theorem 2 from the notes it suffices to look at prime powers.)

b)* Show that for any $k \in \mathbb{Z}^+$ and any real number C , there exists an n such that $d(n) > C(\log n)^k$. (Suggestion: consider $n = (2 \cdot 3 \cdots p_r)^A$, i.e., numbers which are divisible by many small primes to a large power.)

In other words, the divisor function is always smaller than any power of n and is sometimes larger than any power of the logarithm of n .

6.8G: Suppose n and d are positive integers. The natural surjective homomorphism of rings

$$\mathbb{Z}/nd\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

induces a homomorphism of unit groups

$$\iota : (\mathbb{Z}/nd\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times.$$

- Show that ι is itself a surjective homomorphism of abelian groups.
- Explain why this gives another proof of 6.1.
- Is it true that for any surjective ring homomorphism $R \rightarrow S$, the induced homomorphism on unit groups is surjective?