MATH 203, PROBLEM SET 8

DUE THE LAST DAY OF CLASS, APRIL 26.

1. THE MOBIUS FUNCTION

For use in the next group of problems, we need some facts about the mobius \( \mu \) function, which is defined in the following way. Let \( n \geq 1 \) be an integer. If \( n = 1 \), let \( \mu(n) = 1 \). If \( n = p_1 \cdots p_s \) is a product of \( s \geq 1 \) distinct prime numbers \( p_i \), let \( \mu(n) = (-1)^s \). For all other positive integers \( n \), define \( \mu(n) = 0 \). Thus \( \mu(n) = 0 \) if \( n \) is divisible by the square of a prime.

1. Show that if \( n \) and \( m \) are relatively prime positive integers, then
   \[
   \mu(n \cdot m) = \mu(n) \cdot \mu(m).
   \]

2. Show that if \( n \geq 1 \), then \( \sum_{1 \leq d | n} \mu(d) \) equals 1 if \( n = 1 \) and equals 0 if \( n > 1 \).

   Hint: Suppose \( n = p_1^{e_1} \cdots p_s^{e_s} \) for some \( s \geq 1 \) and some distinct primes \( p_i \) and integers \( e_i \geq 1 \). Show that if \( m = p_1 \cdots p_s \) then
   \[
   \sum_{1 \leq d | n} \mu(d) = \sum_{1 \leq t | m} \mu(t).
   \]

   Then show that the set of divisors of \( m \) is the union of the disjoint sets
   \[
   \{t' : 1 \leq t'|(m/p_s)\} = S \quad \text{and} \quad \{t'p_s : t' \in S\}.
   \]

   Consider the contributions of \( t = t' \) and \( t = t'p_s \) to \( \sum_{1 \leq t | m} \mu(t) \).

3. Suppose \( n = p_1^{e_1} \cdots p_s^{e_s} \) as in the hint for problem #2. Show that
   \[
   \sum_{1 \leq d | n} (n/d) \mu(d) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)
   \]

   Hint: Show that the only \( d \) which contribute to the left hand side are products of distinct primes, and expand the product on the right hand side. It may be useful to induct on \( s \).

2. G.C.D.’s

4. Suppose \( F \) is the field \( \mathbb{Z}/3 \). Find the G.C.D. in \( F[x] \) of the polynomials \( a(x) = x^2 + x + 1 \) and \( b(x) = x^3 + x^2 + 1 \). Express this G.C.D. as a linear combination of \( a(x) \) and \( b(x) \).

5. Suppose \( 0 < s, t \in \mathbb{Z} \) and that \( p \) is a prime. Show that in \( (\mathbb{Z}/p)[x] \),
   \[
   G.C.D.(x^s, x^t - 1) = 1.
   \]

   Then show
   \[
   G.C.D.(x^s - 1, x^t - 1) = x^d - 1
   \]
   when \( d = g.c.d.(s, t) \).
(Hint: First check the statements when \( s = t \). Then try to prove them using induction on \( \max(s, t) \). Note that

\[
G.C.D.(a(x), b(x)) = G.C.D.(a(x), b(x) + u(x)a(x))
\]

for all \( a(x), b(x), u(x) \in (\mathbb{Z}/p)[x] \) such that \( a(x) \) and \( b(x) \) are not both 0.)

3. Irreducible Divisors of \( x^r - 1 \) in \( (\mathbb{Z}/p)[x] \).

In this section we will suppose that \( p \) is a prime and that \( r \geq 1 \) is an integer which is relatively prime to \( p \). The goal is to prove the following result, which is needed in the discussion of the polynomial time primality test.

**Theorem 3.1.** There is a monic irreducible polynomial \( h(x) \in (\mathbb{Z}/p)[x] \) which divides \( x^r - 1 \) for which the following is true. Let \( I \) be the ideal \((\mathbb{Z}/p)[x] \cdot h(x)\). Suppose \( z \) and \( z' \) are integers for which \( 0 \leq z < z' < r \). Then \( x^{z'} - x^z \) is not congruent to 0 mod \( I \). Equivalently, the classes \([x^{z'}]\) and \([x^z]\) in the quotient ring \((\mathbb{Z}/p)[x]/I\) are distinct.

6. Suppose \( \pi(x) \) is an irreducible polynomial in \((\mathbb{Z}/p)[x]\) which divides both \( x^r - 1 \) and \( x^{z'} - x^z = x^z(x^{z'-z} - 1) \) for some \( 0 \leq z < z' < r \). Show that \( \pi(x) \) divides \( x^d - 1 \) when \( d = \text{g.c.d.}(r, z' - z) < r \).

Hint: Use Problem #5.

7. Suppose \( \pi(x) \) is an irreducible polynomial in \((\mathbb{Z}/p)[x]\) which divides \( x^d - 1 \) for some \( 1 \leq d \mid r \). Show that \( \pi(x)^2 \) does not divide \( x^d - 1 \).

Hints: Let \( f(x) \in \mathbb{Z}[x] \) be a polynomial which reduces to \( \pi(x) \) mod \( p \). Show that if \( \pi(x)^2 \) divides \( x^d - 1 \) in \((\mathbb{Z}/p)[x]\) then there are polynomials \( g(x), j(x) \in \mathbb{Z}[x] \) such that

\[
(3.1) \quad f(x)^2g(x) = x^d - 1 + p \cdot j(x)
\]

in \( \mathbb{Z}[x] \). Now differentiate both sides of (3.1) using the usual product rule, and reduce the resulting polynomial equation mod \( p \). Using the fact that \( d \mid r \) and \( r \) is prime to \( p \), argue that the reduction \( \pi(x) \) of \( f(x) \) mod \( p \) must divide both \( x^{d-1} \) and \( x^d - 1 \) in \((\mathbb{Z}/p)[x]\). Then use problem #5 to get a contradiction.

8. Let \( \pi(x) \) be an irreducible polynomial dividing \( x^r - 1 \) in \((\mathbb{Z}/p)[x]\). Let \( \Delta(\pi(x)) \) be the smallest divisor \( d \) of \( r \) such that \( \pi(x) \) divides \( x^d - 1 \). Show that if \( d' \geq 1 \) divides \( r \), then \( \pi(x) \) divides \( x^{d'} - 1 \) if and only if \( \Delta(\pi(x)) \mid d' \).

Hint: Use Problem #5.

9. For each irreducible polynomial \( \pi(x) \) of \((\mathbb{Z}/p)[x]\) and each non-zero polynomial \( f(x) \in (\mathbb{Z}/p)[x] \), let \( \text{mult}(\pi(x), f(x)) \) be the largest power of \( \pi(x) \) which divides \( f(x) \). Suppose \( \pi(x) \) divides \( x^r - 1 \). Define \( r' = r/\Delta(\pi(x)) \) for \( \Delta(\pi(x)) \) as in problem #8. Show

\[
(3.2) \quad \sum_{1 \leq d \mid r} \text{mult}(\pi(x), x^d - 1) \cdot \mu(r/d) = \sum_{\Delta(\pi(x)) \mid d'} \mu(r/d) = \sum_{d' \mid r'} \mu(r'/d)
\]

Conclude from Problem #2 that this sum is 1 if \( r' = 1 \) and is 0 if \( r' > 1 \).

Hints: Problem #7 shows that \( \text{mult}(\pi(x), x^d - 1) \) is either 0 or 1 for \( d \mid r \). Now use Problem #8.
10. Let $z(x)$ be the product of all the monic irreducible polynomials $\pi(x)$ which divide $x^r - 1$ but do not divide any polynomial $x^d - 1$ when $d|r$ and $d < r$. Show that
\begin{equation}
\prod_{d|r, \mu(r/d)=1} (x^d - 1) = z(x) \cdot \prod_{d|r, \mu(r/d)=-1} (x^d - 1)
\end{equation}
Hint: Use the multiplicity calculations in problem #9 along with problem #7.

11. Show that $z(x)$ in problem #10 has degree
\begin{equation}
\deg(z(x)) = \left( \sum_{d|r, \mu(r/d)=1} d \right) - \left( \sum_{d|r, \mu(r/d)=1} d \right)
\end{equation}
\begin{equation}
= \sum_{d|r} d \cdot \mu(r/d)
\end{equation}
Use problem #3 to show that this degree is positive. Conclude that $z(x)$ is a non-constant polynomial. Finally, explain why any irreducible factor $h(x)$ of $z(x)$ will satisfy the conditions in Theorem 3.1.

Hint: To show that $h(x)$ will have the right properties, use the definition of $z(x)$ in Problem 10 along with Problem #6.