

MATH 4400
HOMEWORK 4
COMMENTS AND SOLUTIONS

Problem 1: Let f be a multiplicative arithmetic function. Show that f is completely multiplicative if and only if its convolution inverse g is given by the formula $g(n) = \mu(n)f(n)$ for all n .

Solution: First of all, suppose that f is completely multiplicative. Then define $g(n) = \mu(n)f(n)$, and note that

$$(f \star g)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) \mu(d)f(d) = \sum_{d|n} f(n)\mu(d) = f(n) \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

So g is the convolution inverse of f .

For the converse, suppose that $g(n) = \mu(n)f(n)$ is the convolution inverse of f and that f is multiplicative. Then f is completely multiplicative if and only if $f(p^k) = f(p)^k$ for all primes p and positive integers k . (Why is this sufficient?)

Well, the convolution formula gives

$$(f \star g)(p^k) = f(p^k)f(1) - f(p^{k-1})f(p)$$

so $f(p^k) = f(p^{k-1})f(p)$. Then the fact that $f(p^k) = f(p)^k$ follows by an easy induction. \square

Problem 2: Given an arithmetic function $f(n)$, we define the Dirichlet series $F(s)$ of $f(n)$ by the formula

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

(a) Let f and g be two arithmetic functions with associated Dirichlet series F and G . Let s lie in a region in which the series defining F and G converge absolutely. Show that

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f \star g)(n)}{n^s}.$$

(b) Define $\zeta(s)$ to be the Dirichlet series associated to the function **1**. It is well-known that $\zeta(2) = \pi^2/6$. Deduce that

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{6}{\pi^2}.$$

Solution: (a) When we multiply out the product $F(s)G(s)$, we get a bunch of terms of the form $\frac{f(a)g(b)}{a^s b^s}$. We group terms by denominator (we are allowed to rearrange them because of the absolute convergence assumption). So we get

$$F(s)G(s) = \sum_{n=1}^{\infty} \sum_{ab=n} \frac{f(a)g(b)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{ab=n} f(a)g(b),$$

but of course $\sum_{ab=n} f(a)g(b)$ is just $(f \star g)(n)$.

(b) This follows from part (a) plus that fact that $\mu \star \mathbf{1} = \delta$, plus the fact that the Dirichlet series associated to δ is just the constant 1. \square

Problem 3: We have seen that the cyclotomic polynomials $\Phi_n(x)$ are monic irreducible polynomials of degree $\varphi(n)$ with integer coefficients, so they can be written as

$$\Phi_n(x) = x^{\varphi(n)} + c_{\varphi(n)-1}x^{\varphi(n)-1} + \cdots + c_1x + c_0.$$

For some of these problems, it might help to write down the first ten or twenty cyclotomic polynomials.

- (a) Based on your data, make a conjecture about the value of c_0 . Prove it.
- (b) For $n \geq 2$, show that the coefficients of $\Phi_n(x)$ are palindromic; that is, $c_{\varphi(n)-k} = c_k$.
- (c) Based on your data, make a conjecture about the value of c_1 . Prove it.
- (d) Show that $\Phi_{na}(x) | \Phi_n(x^a)$ for all a, n .
- (e) For which a and n is it true that $\Phi_{na}(x) = \Phi_n(x^a)$?

Solution: (a) For $n \geq 2$, c_0 is always 1. Proof: Clearly true for $n = 2$. Now assume $n \geq 3$. Because $\Phi_n(x) = \prod(x - \zeta)$, as ζ runs over the primitive n th roots of unity, we get that c_0 equals $(-1)^{\varphi(n)}$ times the product of all of the primitive n th roots of unity. Since $n \geq 3$, $\varphi(n)$ is even. (See Problem 4 for a very brief discussion of the proof of this fact.) So we are left with the product of ζ_n^a , as a runs over all the elements of $(\mathbb{Z}/n\mathbb{Z})^*$. (Here $\zeta_n = e^{2\pi i/n}$, as usual.) This equals

$$\zeta_n^{\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} a} = \zeta_n^{n\varphi(n)/2},$$

because the elements of $(\mathbb{Z}/n\mathbb{Z})^*$ can be put into $\varphi(n)/2$ disjoint pairs $(a, n-a)$. But this is 1 because $\varphi(n)$ is even.

(b) The first thing to notice is that $\Phi_n(x)$ and $x^{\varphi(n)}\Phi_n(1/x)$ are both polynomials, and they both have the same (non-repeated) roots. This is because ζ is a primitive n th root of unity if and only if $1/\zeta$ is. Ah, but both polynomials have degree $\varphi(n)$, and both are monic (because $c_0 = 1$). So they are equal! But

$$x^{\varphi(n)}\Phi_n(1/x) = c_0x^{\varphi(n)} + c_1x^{\varphi(n)-1} + \cdots + c_{\varphi(n)-1}x + 1.$$

Comparing coefficients with $\Phi_n(x)$, we see that $c_{\varphi(n)-k} = c_k$.

(c) The data seem to indicate that in fact $c_1 = -\mu(n)$. This is true in general, and it is easiest to prove that $c_{\varphi(n)-1} = -\mu(n)$. This is because $c_{\varphi(n)-1}$ is the negative of the sum of the primitive n th roots of unity. So we are reduced to proving that the sum of the primitive n th roots of unity is $\mu(n)$.

How does this work? Well, let $s(n)$ be the sum of the primitive n th roots of unity. We'll show that $s(n)$ is a multiplicative arithmetic function, and then we'll check that $s(n) = \mu(n)$ on prime powers to finish the proof. First, let Z_n be the set of primitive n th roots of unity. Then if a and b are relatively prime, the map $Z_a \times Z_b \rightarrow Z_{ab}$ sending (α, β) to, you guessed it, $\alpha\beta$ is (you guessed it!) a bijection. (Proof left as an exercise, but it's completely straightforward—the hard part is showing that the map actually lands in Z_{ab} .) But then

$$s(a)s(b) = \prod_{\alpha \in Z_a} \prod_{\beta \in Z_b} \alpha\beta = \prod_{\gamma \in Z_{ab}} \gamma = s(ab),$$

so we get multiplicativity.

Now $s(1) = 1$, and $s(p) = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1 = \mu(p)$. What about $s(p^k)$ for $k \geq 2$? Well, let $\omega = e^{2\pi i/p^k}$; then

$$s(p^k) = (1 + \omega + \omega^2 + \cdots + \omega^{p^k-1}) - (1 + \omega^p + \omega^{2p} + \cdots + \omega^{p(p^k-1)})$$

The first sum is invariant under multiplication by ω , so it must be zero; and the second sum is invariant under multiplication by ω^p , which is not 1, so this sum must be zero as well. So we get $s(p^k) = 0 - 0 = 0 = \mu(p^k)$.

(Alternatively, you could derive the statement about the coefficient of Φ_{p^k} by using the work you do in part (e) to note that Φ_{p^k} is a polynomial in x^p , so the coefficient of x must be zero.)

(d) If ζ is a primitive n th root of unity, then ζ^a is a primitive n th root of unity. (This is clear.) So every root of $\Phi_{na}(x)$ is a root of $\Phi_n(x^a)$, and so the result follows because $\Phi_{na}(x)$ has no repeated roots.

(e) The polynomials are equal if and only if their degrees are equal, because they are both monic and one divides the other. So we want that $\varphi(na) = a\varphi(n)$. Well,

$$a\varphi(n) = an \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(an) = an \prod_{\substack{p|an \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

so it looks like this happens if and only if the primes dividing n are exactly equal to the primes dividing an ; that is, if and only if every prime that divides a divides n as well. \square

Problem 4: Find all n such that $\varphi(n) = 12$. Prove that your list is complete!

Solution: Writing n as a product of prime powers, we get that 12 can be written as a product of φ of those prime powers. Notice that it is impossible for $\varphi(a) = 3$ for any a , as $\varphi(a)$ is always even for any $a \geq 3$. (You can either see this from the formula, or from the realization that elements of $(\mathbb{Z}/a\mathbb{Z})^*$ can be put into disjoint pairs $(k, a - k)$.)

So the only possibilities for the factorization of $\varphi(n)$ into the product of φ 's of prime powers are 12, $1 \cdot 12$, $2 \cdot 6$, and $1 \cdot 2 \cdot 6$. So we need to find all prime powers p^k such that $\varphi(p^k) = 1, 2, 6$, or 12.

Well, $\varphi(p^k) = 1$ only happens if $p^k = 2$. That much is clear from the formula. Now suppose $\varphi(p^k) = 2$. Since $\varphi(p^k) = p^{k-1}(p-1)$, we get that either $p^{k-1} = 1$ and $p-1 = 2$, or $p-1 = 1$ and $p^{k-1} = 2$. The first equation leads to $p = 3, k = 1$; the second equation leads to $p = 2, k = 2$. So $p^k = 3$ or 4.

Now suppose $\varphi(p^k) = 6$. We get $p^{k-1}(p-1) = 6$. If $p^{k-1} = 1$ and $p-1 = 6$, we get $p^k = 7$. If $p^{k-1} = 2$ and $p-1 = 3$, we get no solution. If $p^{k-1} = 3$ and $p-1 = 2$, we get $p^k = 9$. If $p^{k-1} = 6$ and $p-1 = 1$, we get no solution. So $p^k = 7$ or 9.

Now suppose $\varphi(p^k) = 12$. We get $p^{k-1}(p-1) = 12$. Clearly p^{k-1} can't be 6 or 12, which aren't prime powers. Listing the remaining cases one by one, we get $p^{k-1} = 1$ and $p-1 = 12$ so $p^k = 13$. Then we try $p^{k-1} = 2$ and $p-1 = 6$; no solution. Then we try $p^{k-1} = 3$ and

$p - 1 = 4$; no solution. Then we try $p^{k-1} = 4$ and $p - 1 = 3$; no solution (remember p has to be prime). So $p^k = 13$.

Putting it all together, we get that if n is a prime power, it's 13. If it's the product of a prime power whose φ is 1 with a prime power whose φ is 12, it must be $2 \cdot 13 = 26$. If it's the product of a prime power whose φ is 2 with a prime power whose φ is 6, we can try 3 or 4 times 7 or 9. Except, wait—we can't do 3 times 9 because those aren't relatively prime. The other three cases give $n = 21, 28, \text{ or } 36$.

Finally, if n is the product of three prime powers whose φ 's are 1, 2, 6 respectively, then n must be 2 times an odd number from the previous paragraph. The only one that qualifies is $n = 2 \cdot 21 = 42$. So our final list is

$$n = 13, 21, 26, 28, 36, 42. \quad \square$$

Problem 5: Show there is a division algorithm in $\mathbb{Z}[x]$ of sorts; more specifically, show that if $a(x)$ and $b(x)$ are polynomials in $\mathbb{Z}[x]$, and $b(x)$ is *monic*, then we can write $a(x) = b(x)q(x) + r(x)$ with $q(x)$ and $r(x)$ in $\mathbb{Z}[x]$, and $\deg r(x) < \deg b(x)$.

Solution: This is an exercise in revisiting the proof of the division algorithm in $F[x]$ where F is a field. In fact this proof does not use the full power of the fact that F is a field; all it requires is that the leading coefficient of $b(x)$ be invertible. So in fact there is a division algorithm of sorts in $R[x]$ for any integral domain R , namely that we can divide $a(x)$ by $b(x)$ in $R[x]$ as long as the leading coefficient of $b(x)$ is in R^* . \square

Problem 6: Find a formula for the convolution inverse of $\sigma_k(n)$.

Solution: Let's do a few prime powers and see what comes up. Notice that the convolution inverse is multiplicative, so it's enough to figure out what it is on prime powers. Let's call the function we're looking for g . Clearly $g(1) = 1$. Now $g(p)\sigma_k(1) + g(1)\sigma_k(p) = 0$, so $g(p) + (p^k + 1) = 0$. So $g(p) = -(p^k + 1)$. Next,

$$\begin{aligned} g(p^2)\sigma_k(1) + g(p)\sigma_k(p) + g(1)\sigma_k(p^2) &= 0 \\ g(p^2) - (p^k + 1)(p^k + 1) + (p^{2k} + p^k + 1) &= 0 \\ g(p^2) &= p^k \end{aligned}$$

Now I won't bore you with $g(p^3)$ and $g(p^4)$, but it turns out they're both 0. (You should verify this at least for $g(p^3)$, as otherwise our proof below will be incomplete.) So that leads to the following guess: $g(1) = 1$, $g(p) = -(p^k + 1)$, $g(p^2) = p^k$, and $g(p^a) = 0$ if $a \geq 3$.

Let's prove our guess by induction. The base case is $a = 3$, which I leave to you. (Actually, you can derive the $a = 3$ case from the work we do below.) Now suppose we've shown it for powers of p up to and including p^{a-1} . Then

$$\begin{aligned} 0 &= g(p^a)\sigma_k(1) + g(p^{a-1})\sigma_k(p) + \cdots + g(p)\sigma_k(p^{a-1}) + g(1)\sigma_k(p^a) \\ 0 &= g(p^a) + p^k\sigma_k(p^{a-2}) - (p^k + 1)\sigma_k(p^{a-1}) + \sigma_k(p^a) \\ -g(p^a) &= p^k \left(\frac{p^{k(a-1)} - 1}{p^k - 1} \right) + (p^k + 1) \left(\frac{p^{ka} - 1}{p^k - 1} \right) - \left(\frac{p^{k(a+1)} - 1}{p^k - 1} \right) \\ g(p^a)(1 - p^k) &= -p^k(p^{k(a-1)} - 1) + (p^k + 1)(p^{ka} - 1) - (p^{k(a+1)} - 1) \\ g(p^a)(1 - p^k) &= -p^{ka} + p^k + p^{k(a+1)} + p^{ka} - p^k - 1 - p^{k(a+1)} + 1 = 0 \end{aligned}$$

so $g(p^a) = 0$ and we are done by induction. All right! So the general formula for g is

$$g(n) = \prod_{\substack{p|n \\ p \text{ prime}}} \begin{cases} -(p^k + 1) & \text{if } p|n \text{ but } p^2 \nmid n \\ p^k & \text{if } p^2|n \text{ but } p^3 \nmid n \\ 0 & \text{if } p^3|n \end{cases}$$

By the way, this formula works for $k = 0$ as well, although you might want to derive it separately, since we were dividing by $p^k - 1$ in the above derivation.

Problem 7: (a) Let p be an odd prime. Show that the following three statements are equivalent:

- (1) p can be written in the form $x^2 + 2y^2$, $x, y \in \mathbb{Z}$
- (2) -2 is a square mod p
- (3) p is not irreducible in the ring $\mathbb{Z}[\sqrt{-2}]$

(b) If we really want to make this look like the theorem we proved in class, there should be a fourth equivalent condition, which should be a congruence condition: p is congruent to something(s) mod something. Make a conjecture as to what that condition should be! We will prove it soon.

Solution: It helps to know that $\mathbb{Z}[\sqrt{-2}]$ has a nice division algorithm, so it's a PID and has unique factorization into irreducibles and all that. (Recall that we define $N(x + y\sqrt{-2})$ to be $x^2 + 2y^2$; this norm is multiplicative and so on, just like it was for the Gaussian integers. Then we can do a division with a remainder that has smaller norm than the thing we divided by.)

So this is just an exercise in translating the Gaussian integer proof over to this ring. I'll illustrate how it goes. To see that (1) implies (2), just write $p = x^2 + 2y^2$ and note that y should not be divisible by p (if it were, then x would be as well, but then the right side would be divisible by p^2 , which is a contradiction). So then considering the equation mod p , we get $x^2 + 2y^2 \equiv 0 \pmod{p}$, so $(x/y)^2 \equiv -2 \pmod{p}$. (Obviously it's important to realize why we can divide by $y \pmod{p}$!)

To see that (2) implies (3), we have that $p|(a^2 + 2)$ for some integer a . Viewing this equation in $\mathbb{Z}[\sqrt{-2}]$, suppose that p were irreducible in $\mathbb{Z}[\sqrt{-2}]$; then p would have to divide either $a + \sqrt{-2}$ or $a - \sqrt{-2}$. But if a rational integer (i.e. an element of \mathbb{Z}) divides $x + y\sqrt{-2}$, it has to divide both x and y . So we get $p|\pm 1$, which is absurd. Hence p is not irreducible in $\mathbb{Z}[\sqrt{-2}]$.

To see that (3) implies (1), write a nontrivial $\mathbb{Z}[\sqrt{-2}]$ -factorization of p : $p = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, both non-units. Take norms to get $p^2 = N(\alpha)N(\beta)$. Norms of things in $\mathbb{Z}[\sqrt{-2}]$ are always positive, and of course if $N(\alpha) = 1$ then α is a unit (indeed $\alpha\bar{\alpha} = 1$), so the only way this factorization can be nontrivial is if $N(\alpha) = N(\beta) = p$. If $\alpha = x + y\sqrt{-2}$, then we get that $p = x^2 + 2y^2$.

Hopefully this proof should have looked extremely familiar!

(b) If you generated enough data, you should have come up with the condition $p \equiv 1$ or $3 \pmod{8}$. In fact, now that you know quadratic reciprocity, you can prove that -2 is a square mod p if and only if $p \equiv 1$ or $3 \pmod{8}$. This is because $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$, and now take cases mod 8:

If $p \equiv 1 \pmod{8}$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = 1$, so $\left(\frac{-2}{p}\right) = 1$.

If $p \equiv 3 \pmod{8}$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{2}{p}\right) = -1$, so $\left(\frac{-2}{p}\right) = 1$.

If $p \equiv 5 \pmod{8}$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$, so $\left(\frac{-2}{p}\right) = -1$.

If $p \equiv 7 \pmod{8}$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{2}{p}\right) = 1$, so $\left(\frac{-2}{p}\right) = -1$.

There you go. \square