Number Theory Homework V

RDB

August 17, 2021

This is likely our last homework! Homework is the most important part of our class. I hope that these assignments have been enlightening and fun. To commemorate the occasion, I have produced an *extra fun* homework assignment. Once more unto the breach, dear students.

Exercise 1 Let f be a multiplicative function. That is, $f(ab) = f(a)f(b)$ whenever $\gcd(a, b) = 1$. Prove that $f(1) = 1$, or $f = 0$.

Solution 1
If $f(x_0) \neq 0$ for some integer x_0, then $f(x_0) = f(1 \cdot x_0) = f(1)f(x_0)$ since $\gcd(1, x_0) = 1$ for all x_0. Therefore $f(1) \neq 0$. But also $f(1) = f(1 \cdot 1) = f(1)^2$, so dividing by $f(1)$ gives $f(1) = 1$.

Exercise 2 Prove or provide a counterexample to the following statement: If n is composite, then $\gcd(n, \phi(n)) > 1$.

Solution 2
The smallest counterexample is $n = 15$, since $\phi(15) = 8$ and $\gcd(15, 8) = 1$.

Numbers n such that $\gcd(n, \phi(n)) = 1$ are called *cyclic*. It turns out that n is cyclic iff it is the product of distinct primes $p_1 p_2 \cdots p_r$ where no p_i divides any $p_j - 1$. For example, $n = 2 \cdot 3$ is *not* cyclic, because 2 divides $3 - 1$, but $n = 3 \cdot 5$ *is*, because 3 does not divide $5 - 1$ and 5 does not divide $3 - 1$.

Exercise 3

(**a**) Let f and g be two multiplicative functions. Prove that $f = g$ iff $f(p^k) = g(p^k)$ for all prime powers p^k.

(**b**) Prove that

$$\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}.$$

[Hint: Both sides are multiplicative (why?).]

Solution 3

(**a**) If $f = g$ then obviously $f(p^k) = g(p^k)$ for all prime powers p^k. On the other hand, if $f(p^k) = g(p^k)$, then any integer n can be written in terms of its prime factorization $n = p_1^{e_1} \cdots p_r^{e_r}$, and

$$\begin{aligned} f(n) &= f(p_1^{e_1}) \cdots f(p_r^{e_r}) \\ &= g(p_1^{e_1}) \cdots g(p_r^{e_r}) \\ &= g(n), \end{aligned}$$

since f and g are multiplicative.

(**b**) First, note that the left-hand side is multiplicative. If a and b are relatively prime, then

$$\frac{ab}{\phi(ab)} = \frac{a}{\phi(a)} \frac{b}{\phi(b)}.$$

Similarly, $\mu^2(d)/\phi(d)$ is multiplicative, so by the divisor-sum theorem, this implies that $\sum_{d|n} \mu^2(d)/\phi(d)$ is as well. Therefore, by the previous part, it suffices to check the identity when $n = p^k$ is a prime power.

If $n = p^0 = 1$, then the equation reads

$$\frac{1}{\phi(1)} = \frac{\mu^2(1)}{\phi(1)},$$

which is true. If $n = p$, then the equation reads

$$\frac{p}{\phi(p)} = \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)},$$

which is true since $\phi(p) = p - 1$ and $\mu^2(p) = 1$. Finally, if $n = p^k$ with $k \geq 2$, then the left-hand side is

$$\frac{p^k}{\phi(p^k)} = \frac{p^k}{p^k - p^{k-1}} = \frac{p}{p-1},$$

while the right-hand side is

$$\frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + 0 = 1 + \frac{1}{p-1} = \frac{p}{p-1}.$$

Since both sides are multiplicative and equal on prime powers, they are equal everywhere.

Exercise 4 Prove that $\phi(n)$ is even for $n \geq 3$.

Solution 4
Suppose that n is divisible by some odd prime p with exponent e_p. That is, $n = p^{e_p} n'$, where p does not divide n'. Then

$$\phi(n) = (p^{e_p} - p^{e_p - 1})\phi(n'),$$

and $p^{e_p} - p^{e_p-1}$ is even since p is odd.

If n is divisible by no odd primes, then $n = 2^k$ for some integer k, and we have

$$\phi(n) = 2^{k-1},$$

which is even unless $k = 1$. But if $n \geq 3$, then k is at least 2. Therefore $\phi(n)$ is even for $n \geq 3$.

Exercise 5 Compute

$$\sum_{d \mid 10^{10000}} \phi(d).$$

Solution 5
Since

$$\sum_{d \mid n} \phi(d) = n,$$

$$\sum_{d \mid 10^{10000}} \phi(d) = 10^{10000}.$$

Exercise 6 This exercise involves programming.

Let

$$A(n) = \frac{1}{n} \sum_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} k$$

be the *average integer relatively prime to n*.

(**a**) Write a program `avgRelPrime(n)` which computes the average integer relatively prime to n. (Note that $A(n)$ is not necessarily an integer.)

(**b**) Compute $A(n)$ for $3 \leq n \leq 20$. Look these numbers up in the OEIS. What entry do you find? Can you formulate a conjecture involving $A(n)$ and an arithmetic function we've discussed in class?

Solution 6

(**a**) Here's a relatively simple program:

```
from math import gcd
def avgRelPrime(n):
    s = sum(k for k in range(1, n + 1) if gcd(n, k) == 1)
    return s // n
```

It turns out that $A(n)$ *is* an integer, so we're justified in integer dividing by n.

(**b**)
```
>>> [avgRelPrime(k) for k in range(3, 21)]
[1, 1, 2, 1, 3, 2, 3, 2, 5, 2, 6, 3, 4, 4, 8, 3, 9, 4]
```

When I look these up in the OEIS, I get A23022, which seems to be the *half-totient function.* In other words, I conjecture that

$$A(n) = \frac{\phi(n)}{2}.$$

Amazingly, this is true!

Exercise 7 Given a multiplicative function f, the *Bell series of f with respect to p*, or simply the *Bell series of f*, is defined as

$$f_p(x) = \sum_{k \geq 0} f(p^k)x^k.$$

(**a**) Prove that

$$\mu_p(x) = 1 - x.$$

(**b**) Prove that $(\mu^2)_p(x) = 1 + x$.

(**c**) Let $u(n) = 1$ for all $n \geq 1$. Prove that

$$u_p(x) = \frac{1}{1-x}.$$

(**d**) Prove that the coefficient on x^n in $f_p(x)g_p(x)$ is $\sum_{j=0}^{n} f(p^j)g(p^{n-j})$.

Solution 7

(**a**) Since $\mu(1) = 1$, $\mu(p) = -1$, and $\mu(p^k) = 0$ for $k \geq 2$, we have

$$\mu_p(x) = \sum_{k \geq 0} \mu(p^k)x^k = 1 - x + 0 = 1 - x.$$

(**b**) This is the same as the previous part, except $\mu^2(p) = 1$.

(**c**) This is just the geometric series formula:

$$u_p(x) = \sum_{k \geq 0} u(p^k)x^k = \sum_{k \geq 0} x^k = \frac{1}{1-x}.$$

(**d**) A power of x^n is achieved in $f_p(x)g_p(x)$ by multiplying a term of the $f(p^i)x^i$ with a term of the form $g(p^{n-i})x^{n-i}$, where $0 \leq i \leq n$. Adding all of these terms together gives that the coefficient on x^n is

$$\sum_{j=0}^{n} f(p^j)g(p^{n-j}).$$

Exercise 8 Let $v(n)$ be the number of distinct prime factors of n.

(**a**) Prove that $b(n) = 2^{v(n)}$ is multiplicative.

(**b**) Prove that the Bell series of b is

$$b_p(x) = \frac{1+x}{1-x} = (\mu^2)_p(x)u_p(x)$$

Solution 8

(**a**) If r and s are relatively prime, then they share no prime factors. Therefore $v(rs) = v(r) + v(s)$, which gives

$$b(rs) = 2^{v(rs)} = 2^{v(r)}2^{v(s)} = b(r)b(s),$$

so b is multiplicative. [In fact, $t^{v(n)}$ is multiplicative for *any* real t.]

(**b**) Note that $v(1) = 0$ and $v(p^k) = 1$ for $k \geq 1$, so

$$b_p(x) = 1 + \sum_{k\geq 1} 2^1 x^k.$$

This simplifies as follows:

$$\begin{aligned} 1 + \sum_{k\geq 1} 2x^k &= 1 + 2(\sum_{k\geq 0} x^k - 1) \\ &= 1 + 2\left(\frac{1}{1-x} - 1\right) \\ &= 1 + \frac{2x}{1-x} \\ &= \frac{1+x}{1-x}. \end{aligned}$$

Then, since $(\mu^2)_p(x) = 1 + x$ and $u_p(x) = 1/(1-x)$, it's obvious that

$$b_p(x) = (\mu^2)_p(x)u_p(x).$$