MAT 302: LECTURE SUMMARY

Recall from last lecture that we were trying to prove that $\varphi(n)$ is a *multiplicative* function, i.e. that $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $(m,n) = 1$. We had realized that this would follow from finding a bijection between $\mathbb{Z}_{mn}^\times$ and $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$. Following a suggestion of Kiavash, we set out to prove that the map

$$\begin{aligned} \kappa \ : \ \mathbb{Z}_{mn}^\times &\longrightarrow \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times \\ a &\longmapsto \Big(a \ (\mathrm{mod}\ m), a \ (\mathrm{mod}\ n)\Big) \end{aligned}$$

is a bijection. We proved that it was injective last time, so it remained only to show surjectivity. In other words, given any $(a,b) \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, we wish to find an $x \in \mathbb{Z}_{mn}^\times$ such that $\kappa(x) = (a,b)$. Actually, we don't even need to find this x explicitly: we just need to show that such an x exists.

Let's translate this into a more concrete question. We are looking for an $x \in \mathbb{Z}_{mn}^\times$ such that

$$\begin{aligned} x &\equiv a \ (\mathrm{mod}\ m) \quad \text{and} \\ x &\equiv b \ (\mathrm{mod}\ n) \end{aligned} \tag{1}$$

The trick is to realize that for any number of the form $x_0 = (\quad)m + (\quad)n$, reducing $(\mathrm{mod}\ m)$ or $(\mathrm{mod}\ n)$ kills one of the two terms. In our case, a good choice is

$$x_0 = bm^{-1}m + an^{-1}n$$

where m^{-1} denotes the inverse of $m \ (\mathrm{mod}\ n)$ in the group $\mathbb{Z}_n^\times$, and similarly for n^{-1}. It is easily checked that x_0 simultaneously satisfies both congruences (1). This is promising, but we're not quite done yet: we need a solution in $\mathbb{Z}_{mn}^\times$, whereas x_0 is some random integer we've constructed. This is easy to fix, however. First, since adding any multiple of mn to x_0 yields another solution to (1), we see that $x = x_0 \ (\mathrm{mod}\ mn)$ is a solution in $\mathbb{Z}_{mn}$. Moreover, since $(x_0, mn) = 1$ (why is this?), our lemma from last time implies that $x \in \mathbb{Z}_{mn}^\times$. This completes the proof that κ is a surjective map, and therefore, that it is bijective. It follows that $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $(m,n) = 1$. (Where in the proof did we use that m and n are relatively prime?)
QED

Having proved that $\varphi(n)$ is multiplicative, we generated some other examples of multiplicative functions. A simple example is the identity map $I(n) = n$. Actually, this function is not just multiplicative, but is also *completely multiplicative*: $I(mn) = I(m)I(n)$ for *any* m and n, independent of whether or not they are relatively prime to each other. Other examples of completely multiplicative functions we discussed were $\mathbb{1}(n) = 1$, $f(n) = n^2$,

$$\chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \ (\mathrm{mod}\ 4) \\ -1 & \text{if } n \equiv -1 \ (\mathrm{mod}\ 4) \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Date: February 17th, 2011.

We also saw that we could 'force' complete multiplicativity by defining a function appropriately: we defined a function λ by setting $\lambda(1) = 1$, $\lambda(p) = -1$ for every prime p, and extending λ to all integers by setting $\lambda(mn) = \lambda(m)\lambda(n)$ for every m and n. For example,

$$\lambda(12) = \lambda(2 \times 2 \times 3) = \lambda(2)\lambda(2)\lambda(3) = -1.$$

Thus, $\lambda(n)$ is completely multiplicative by definition. Finally, we talked a bit about a related function, $\mu(n)$, defined by $\mu(1) = 1$, $\mu(n) = \lambda(n)$ whenever $n = p_1 p_2 \cdots p_k$ for some collection of distinct primes p_i, and 0 otherwise. For example, $\mu(6) = \lambda(6) = 1$, while $\mu(12) = 0$ (since 12 cannot be written as the product of distinct prime factors). In your problem set, you will explore the multiplicativity of $\mu(n)$.

We ended the lecture with a brief discussion of a familiar and important result about factorization of integers into primes:

Theorem 1 (Fundamental Theorem of Arithmetic, informal version)**.** *Any positive integer can be factored in a unique way as a product of prime numbers.*

There are several issues with this statement. First, what does 'unique' mean? For example, $6 = 2 \times 3 = 3 \times 2$. Second, how does the theorem apply to the positive integer 1? It is standard to not consider 1 as a prime, in which case it is not clear how to write it as a product of primes, uniquely or otherwise. If we instead decide to call 1 a prime, then uniqueness begins to fail even more dramatically than above: $6 = 2 \times 1 \times 3 \times 1$ would be considered a 'new' factorization of 6. (Actually this is one of the reasons why mathematicians *don't* consider 1 to be prime.)

These difficulties force us to state the fundamental theorem in an uglier (but more precise) way.

Theorem 2 (Fundamental Theorem of Arithmetic, precise version)**.** *Given any positive integer n, there exists a unique sequence $n_2, n_3, n_5, n_7, n_{11}, \ldots \in \mathbb{N}$ such that*

$$n = \prod_p p^{n_p}$$

where the product runs over all primes p.

For example, we have the following factorizations:

$$\begin{aligned}
1 &= 2^0\,3^0\,5^0\,7^0\,11^0 \cdots \\
3 &= 2^0\,3^1\,5^0\,7^0\,11^0 \cdots \\
6 &= 2^1\,3^1\,5^0\,7^0\,11^0 \cdots \\
9 &= 2^0\,3^2\,5^0\,7^0\,11^0 \cdots \\
18 &= 2^1\,3^2\,5^0\,7^0\,11^0 \cdots
\end{aligned}$$

This notation is obviously somewhat redundant, but has the advantages of being precise and quite useful. We ended the class by exploring this notation.

Proposition 3. *$d \mid n$ if and only if $d_p \leq n_p$ for every prime p.*

Proposition 4.

$$(a,b) = \prod_p p^{\min\{a_p, b_p\}}$$

(Can you prove these propositions?)

Theorem 5. *Suppose* $(m,n) = 1$ *and* $d \mid mn$*. Then* $(d,m) \times (d,n) = d$*.*

Proof. First, by Proposition 4, we have

$$(d,m) \times (d,n) = \prod_p p^{\min\{d_p, m_p\} + \min\{d_p, n_p\}}.$$

Proposition 3 tells us that $d_p \leq m_p + n_p$ for each p. Since $(m,n) = 1$, we see (from the uniqueness part of the Fundamental Theorem and Proposition 4) that for each p, either m_p or n_p must be 0. Suppose $m_p = 0$ for some particular prime p. Then $d_p \leq n_p$, whence

$$\min\{d_p, m_p\} + \min\{d_p, n_p\} = d_p.$$

The same holds true if instead $n_p = 0$. Since either m_p or n_p must be zero for every prime p, we conclude that

$$(d,m) \times (d,n) = \prod_p p^{d_p} = d$$

□