Manuel Kauers
RISC-Linz

Hagenberg, June 14, 2004

Algorithmic Combinatorics

Homework 11

Exercise 1 If $n, m \in \mathbb{Z}$ are coprime, then

$$\varphi(nm) = \varphi(n) \cdot \varphi(m).$$

Let $n, m \in \mathbb{Z}$ be coprime. Then the ideals $(n), (m) \trianglelefteq \mathbb{Z}$ are coprime, because the Euclidean algorithm asserts the existence of numbers $a, b \in \mathbb{Z}$ with

$$an + bm = \gcd(n, m) = 1.$$

Now, by the Chinese remainder theorem,

$$\mathbb{Z}/(n) \cap (m) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m).$$

If these rings are isomorphic, then in particular also their multiplicative groups are:

$$\left(\mathbb{Z}/(n) \cap (m)\right)^* \cong \left(\mathbb{Z}/(n)\right)^* \times \left(\mathbb{Z}/(m)\right)^*.$$

Observing that $(n) \cap (m) = (nm)$ and that for every $N \in \mathbb{Z}$,

$$\varphi(N) = |\{\, k \in [N] : k \perp N \,\}| = \left|\left(\mathbb{Z}/(N)\right)^*\right|$$

(again by Euclid) completes the proof.

Exercise 2 For all $n \in \mathbb{N}$,

$$\varphi(n) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Let $N = p_1^{e_1} \dots p_r^{e_r}$ be a prime decomposition of N. For every prime p_i, we obviously have

$$\varphi(p_i^{e_i}) = \left|\left(\mathbb{Z}/(p_i^{e_i})\right)^*\right| = p_i^{e_i} - p_i^{e_i}/p_i = p_i^{e_i - 1}(p_i - 1).$$

Furthermore, $p_i^{e_i} \perp p_j^{e_j}$ for $i \neq j$. Iterated application of Exercise 1 gives

$$\prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = \prod_{i=1}^{r} p_i^{e_i}(1 - 1/p_i) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Exercise 3 For all $n \in \mathbb{N}$,

$$n = \sum_{d \mid n} \varphi(d).$$

Write $n = p_1^{e_1} \dots p_r^{e_r}$. We proceed by induction on r. For $r = 0$, we have $n = 1$ and

$$\sum_{d|1} \varphi(d) = \varphi(1) = 1.$$

Suppose the claim holds for $r \in \mathbb{N}$, i.e. for all $n \in \mathbb{N}$ with at most r different prime factors. Let n be such a number, p be a "new" prime, and $e \in \mathbb{N}$. We prove the claim for np^e. First,

$$\sum_{d|np^e} \varphi(d) = \sum_{d|n} \sum_{i=1}^{e} \underbrace{\varphi(dp^i)}_{\varphi(d)\varphi(p^i)} = \underbrace{\sum_{d|n} \varphi(d)}_{=n} \cdot \sum_{i=0}^{e} \varphi(p^i).$$

Concerning the last sum, we find

$$\sum_{i=0}^{e} \varphi(p^i) = 1 + \sum_{i=1}^{e} p^i(1 - 1/p) = 1 + \sum_{i=1}^{e} \left(p^i - p^{i-1}\right) = 1 + p^e - 1 = p^e.$$

Putting things together, we obtain

$$\sum_{d|np^e} \varphi(d) = np^e,$$

as required.