L 20 (May 4, 2020) Let $f \in \mathbb{Z}_p[x]$ be an irreducible polynomial with $\deg(f) = n \in \mathbb{N}$. We may assume that $f$ is <u>monic</u>, i.e. $f = f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ with $a_i \in \mathbb{Z}_p$ ($f(x)$ has leading coefficient $1_{\mathbb{Z}_p}$). We take the ideal $I = (f) = \{rf \mid r \in \mathbb{Z}_p[x]\}$ generated by $f$. In one of the previous lectures we proved that $I$ is a maximal ideal. Another result we proved implies that $\mathbb{Z}_p[x]/I$ is a field. What is $|R|$?

$R :=$

**Problem 20.1.** Prove that the elements of the factor-ring $R = \mathbb{Z}_p[x]/(f)$ (*) one-to-one correspond to the polynomials $g \in \mathbb{Z}_p[x]$ with $\deg(g) < n$ and (to) $g = 0_{\mathbb{Z}_p[x]}$, i.e. to $g = g(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1 x + b_0$, $b_i \in \mathbb{Z}_p$.

Hence $|R| = |\mathbb{Z}_p[x]/I| = p^n$ and $R$ is a field with $p^n$ elements. □

I finished the proof here but, of course, we have to prove that $\forall n \in \mathbb{N}$ there is an irr. polynomial in $\mathbb{Z}_p[x]$ with degree $n$. This is the long

(*) ~~which is a field~~. For our $f$.

time ago promised nice connection of enumerative combinatorics and algebra. We in fact derive a formula for the number $a_n$ of such polynomials, and the formula will show that $a_n \geq 1$ for any $n \in \mathbb{N}$. To be precise, we set, for fixed prime $p$ and $n \in \mathbb{N}$,

$$a_n = |\{f \in \mathbb{Z}_p[x] \mid f \text{ is monic, } f \text{ is irr. and } \deg(f) = n\}|.$$

**Problem 20.2** Prove that two polynomials $f, g \in \mathbb{Z}_p[x]$ are associated $\Leftrightarrow$ $\Leftrightarrow$ $f = gh$ for some $h \in \mathbb{Z}_p[x]$ with $\deg(h) = 0$ (so $h \neq 0_{\mathbb{Z}_p[x]}$).

We also denote by $b_n$ $n \in \mathbb{N}_0$, the # of all monic polynomials in $\mathbb{Z}_p[x]$ with degree $n$: $b_n = |\{f \in \mathbb{Z}_p[x] \mid \deg(f) = n \text{ and } f \text{ is monic}\}|$. It is trivial but I still leave it for you as an exercise: **Problem 20.3** Show that $b_n = p^n$. Here $n = 0, 1, 2, \ldots$

To deduce a formula for $a_n$ (defined above) we consider the generating functions $A(x)$ and $B(x)$ of the sequences $(a_n) = (a_0, a_1, a_2, \ldots)$ and $(b_n) = (b_0, b_1, \ldots)$

$$A(x) = \sum_{n=1}^{\infty} a_n x^n \text{ and } B(x) = \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} p^n x^n =$$

$$= \frac{1}{1-px}$$ (we just summed the formal geometric series).

↑ Pr. 20.3 have

**Theorem** We have the identity:

$$\frac{1}{1-px} = B(x) = \prod_{q=1}^{\infty} \frac{1}{(1-x^q)^{a_q}}.$$

(*)

**Proof.** Now I see that we actually do not and will not need the GF $A(x)$. This identity is just the reflection (in the i. domain of formal power series $\mathbb{Z}[\![x]\!]$ with variable $x$ and coefficients in $\mathbb{Z}$) of the fact that $\mathbb{Z}_p[y]$ is a UFD, which we proved last time in a more general form. Indeed, because $\mathbb{Z}_p[y]$ is a UFD and because of P. 20.2 we have: every monic $f \in \mathbb{Z}_p[y]$ has a unique expression as

$$f = g_1^{a_1'} g_2^{a_2'} \cdots g_r^{a_r'}$$ ($a_i'$ is different from $a_i$!)

where $r \in \mathbb{N}_0$, $a_i' \in \mathbb{N}$ and $g_1, g_2, \ldots, g_r$ are mutually distinct monic irreducible polynomials in $\mathbb{Z}_p[y]$; for $r=0$ we define the right side as "$1_{\mathbb{Z}_p[y]}$" = "$1_{\mathbb{Z}_p}$". the left side of (*) counts the $f$

in $\boxed{\cdots}$ and the right side of (*) counts the right side of $\boxed{\cdots}$. Indeed, the # of $g$ with $\deg(g) = n \in \mathbb{N}_0$ is the coeff. of $x^n$ in $B(x)$, and the coeff. of $x^n$ in $\prod_{q=1}^{\infty} \frac{1}{(1-x^q)^{a_q}} =$

$= \prod_{q=1}^{\infty} \left( \sum_{m=0}^{\infty} x^{qm} \right)^{a_q}$ is the number of ways how to write $n$ in the form

$$\boxed{n = c_1 + c_2 + c_3 + \cdots + c_s} \quad (c_i \in \mathbb{N}_0)$$

where $s \in \mathbb{N}_0$, $c_1 \geq c_2 \geq \cdots \geq c_s$ and $c_i \in \mathbb{N}^C$, where $\mathbb{N}^C$ denotes the set of "colored" natural numbers – each $q \in \mathbb{N}^C$ comes in one of $\boxed{a_q \text{ colors}}$ – these are so called colored partitions of $n$; comparing the degrees in $\boxed{\cdots}$ we get

$$n = \deg(g) = \sum_{i=1}^{\infty} d_i \underbrace{\deg(q_i)}_{\text{this number comes in } a_i \text{ colors}}$$

and these are exactly the colored partitions of $n$. ☒

---

the last step is to invert the identity in order to get a formula for the numbers $a_q$. We take the logarithmic derivative $[x(\log(\cdots))']$ of it:

$$x\left(\log\frac{1}{1-px}\right)' = x\left(\sum_{n=1}^{\infty}\frac{p^n x^n}{n}\right)' \times \frac{B(x)'}{B(x)} =$$

$$= x\cdot\frac{\frac{p}{(1-px)^2}}{\frac{1}{1-px}} = \frac{px}{1-px} = px+(px)^2+(px)^3+\cdots.$$

$$x\left[\log\left(\prod_{n=1}^{\infty}\underbrace{\frac{1}{(1-x^n)^{a_n}}}_{S_n(x)}\right)\right]' = x\sum_{n=1}^{\infty}\frac{S_n(x)'}{S_n(x)} =$$

$$= \sum_{n=1}^{\infty}\frac{a_n n x^n}{\frac{(1-x^n)^{a_n+1}}{(1-x^n)^{a_n}}} = \sum_{n=1}^{\infty}\frac{n a_n x^n}{1-x^n} =$$

$$= \sum_{n=1}^{\infty} n a_n \left(x^n + x^{2n} + x^{3n} + \cdots\right).$$

Comparing the coeffs. of $x^n$ for $n\in\mathbb{N}$ in ⌐ and ⌙, we get the formula

$$\boxed{p^n = \sum_{d\mid n} d\,a_d.}$$

To invert this formula expressing $a_d$ we use the following result from elementary number theory. Recall that the Möbius function

$\mu:\mathbb{N}\to\{-1,0,1\}$ is defined as $\mu(1)=1$, $\mu(p_1p_2\cdots p_r)=(-1)^r$ for distinct primes $p_i$,

and $\mu(n)=0$ else. We have the M. inversion formula: **Proposition** If $f,g:\mathbb{N}\to\mathbb{R}$ functions are such that $\forall n\in\mathbb{N}: f(n)=\sum_{d,d|n} g(d)$, then $\forall n\in\mathbb{N}: g(n)=\sum_{d,d|n}\mu(d) f(\frac{n}{d})$. I do not have time for proof, which is not hard. We apply M. inversion to (6) and get: $\forall n\in\mathbb{N}$,

$$n a_n = \sum_{d,d|n} \mu(d)\, p^{n/d}.$$

So we get the desired formula

$$\boxed{a_n = \frac{1}{n}\sum_{d|n}\mu(d)\,p^{n/d}.}$$

We indeed have that $a_n \geq \frac{1}{n}(p^n - p^{n-1} - \dots - p^1) > 0$ and $\forall n\in\mathbb{N}\ \exists$ irr. $f\in\mathbb{Z}_p[x]$ with $\deg(f)=n$.

---

**Example** The # of monic irr. $f\in\mathbb{Z}_5[x]$ with $\deg(f)=6$ is $\frac{1}{6}\sum_{d|6}\mu(d)\,5^{6/d} = \frac{1}{6}(5^6 - 5^3 - 5^2 + 5^1) = \frac{5}{6}(5^5 - 5^2 - 5^1 + 1) = \frac{5}{6}(3125-25-4)$

$= \frac{5}{6}\,3096 = 5\cdot 516 = \underline{2580}.$

From now we continue with topology!