MATH 3360 PRELIM #2, SPRING 2018, WITH ANSWERS

If two questions have the same number, they concern the same object. For example, the ring in 2b is the one defined in 2. [5π] indicates that a problem is worth 5π points.

---

1 [15]. Let $a, b \in \mathbb{F}_p$ and consider the polynomial $f(x) = x^{2p} + ax + b \in \mathbb{F}_p[x]$.
Assume $\mathbb{E} \geq \mathbb{F}_p$ is a field big enough that $f(x)$ factors into linear factors in $\mathbb{E}[x]$.
How many distinct roots does $f(x)$ have (in $\mathbb{E}$)?

Answer. We had a way to find the repeated roots: look at the GCD of f with its derivative, $2px^{2n-1} + a = a$ (notice $p = 0$). If $a \neq 0$, then this GCD is the unit a, so there are no repeated roots – the answer is 2p distinct roots.

Now assume $a = 0$, and let y be a root, i.e. $y^{2p} = -b$. Then

$$x^{2p} + b = x^{2p} - y^{2p} = (x^2 - y^2)^p \qquad \text{by the Freshman's Dream}$$

so the only roots are those of $x^2 - y^2$, namely $\pm y$.

How many roots is that? If $p = 2$, then $y = -y$, so the polynomial has only one root. Otherwise it has two.

---

2. Let R be a commutative ring. We'll want to define $\mathrm{frac}(R)$ as the equivalence classes of a certain equivalence relation on $F := \{(n, d) \in R^2 \ : \ d \text{ is neither } 0 \text{ nor a zero divisor}\}$:

$$(n_1, d_1) \sim (n_2, d_2) \qquad \Longleftrightarrow \qquad n_1 d_2 = n_2 d_1$$

2a [20]. Prove that this is indeed an equivalence relation on F.

Answer.

Reflexivity and symmetry are both really obvious: the first says $nd = nd$, the second says $n_1 d_2 = n_2 d_1 \iff n_2 d_1 = n_1 d_2$.

What's left is transitivity.

$$(n_1, d_1) \sim (n_2, d_2) \sim (n_3, d_3) \qquad \Longrightarrow \qquad n_1 d_2 = n_2 d_1, n_2 d_3 = n_3 d_2.$$

Hence $(n_1 d_2) d_3 = (n_2 d_1) d_3 = d_1 (n_2 d_3) = d_1 (n_3 d_2)$. Since d_2 is not a zero divisor, $n_1 d_3 = d_1 n_3$.

2b [15]. With more work, one could show that there's a natural ring structure on $\mathrm{frac}(R)$. But don't bother.

Consider the function (which, you may assume, is actually a ring homomorphism)

$$R \to \mathrm{frac}(R), \quad r \mapsto \text{ equivalence class of } (r, 1).$$

If R is finite, prove this is an isomorphism.

Answer. First, we check if it's 1 : 1. If $(r, 1) \sim (s, 1)$, then $r1 = s1$ so $r = s$; yes it's 1 : 1 (this doesn't depend on the finiteness).

For onto: say we have the equivalence class of (n, d), and we want to find some r mapping to it, i.e. $(r, 1) \sim (n, d)$, also known as $rd = n$. This means, evidently, that we want to divide by d.

Consider the multiplication map $d\cdot : R \to R$. Since d is not a zero divisor, it's $1:1$. Since R is finite, this $1:1$ self-map is onto. So it hits n, i.e. $\exists r$ with $dr = n$.

2c [5]. Give an example of an R for which $R \to \mathrm{frac}(R)$ is not an isomorphism.

Answer. We need an infinite ring R that isn't a field. $\mathbb{Z}$ will do; $\mathrm{frac}(\mathbb{Z}) \cong \mathbb{Q}$ and the map $\mathbb{Z} \to \mathbb{Q}$ isn't an isomorphism.

---

3 [20]. Let $n = 2^5 \cdot 5 \cdot 17^4$.
List all pairs $(a, b) \in \mathbb{N}^2$ such that $\mathbb{Z}_n \cong \mathbb{Z}_a \times \mathbb{Z}_b$, and prove your list is complete.

Answer. By CRT, we need $\gcd(a, b) = 1$. So for each of the primes $2, 5, 17$ in n, all of them are in a, or all are in b. That gives 2^3 possibilities:

$(2^5{\cdot}5{\cdot}17^4, 1), (2^5{\cdot}5, 17^4), (2^5{\cdot}17^4, 5), (2^5, 5{\cdot}17^4), (5{\cdot}17^4, 2^5), (5, 2^5{\cdot}17^4), (17^4, 2^5{\cdot}5), (1, 2^5{\cdot}5{\cdot}17^4)$

---

4. Fun fact! The group $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ has five different subgroups:

$$
\begin{array}{ccccccc}
 & & \mathbb{Z}_2 \times \mathbb{Z}_2 & & & & \text{of size 4} \\
 & / & | & \backslash & & & \\
\{(0,0),(1,0)\} & & \{(0,0),(1,1)\} & & \{(0,0),(0,1)\} & & \text{each of size 2, but different subsets} \\
 & \backslash & | & / & & & \\
 & & \{(0,0)\} & & & & \text{of size 1}
\end{array}
$$

Now let's have the actual question.

Let $p, q \in \mathbb{N}$ be prime numbers.

4a [10]. How many different *sizes* of subgroups does $\mathbb{Z}_p \times \mathbb{Z}_q$ have?

Answer.

By Lagrange's theorem, the only options are the divisors of $\#(\mathbb{Z}_p \times \mathbb{Z}_q) = pq$. If $p \neq q$, those are $1, p, q, pq$, and all actually arise (from $\{(0,0)\}$, $\{(a,0) : a \in \mathbb{Z}_p\}$, $\{(0,b) : b \in \mathbb{Z}_q\}$, $\mathbb{Z}_p \times \mathbb{Z}_q$). So four sizes, in that case.

If $p = q$, then the only divisors are $1, p = q, p^2$, so three sizes.

4b [15]. How many *different subgroups* does $\mathbb{Z}_p \times \mathbb{Z}_q$ have?

Answer.

If $p \neq q$, then CRT applies, so $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. The only subgroup of that group of size p is the multiples of q, and vice versa. So there are only four subgroups, one of each possible size.

If $p = q$ as in the fun fact, it's trickier to count the subgroups. Every element g of $\mathbb{Z}_p \times \mathbb{Z}_p$ other than $(0,0)$ is of order p, so generates a (cyclic) subgroup of size p. Inside that group $\{(0,0), g, 2g, \ldots, (p-1)g\} \cong \mathbb{Z}_p$, every element except $(0,0)$ is a generator of that subgroup. So there are $p-1$ elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ generating the same subgroup. This gives $(p^2-1)/(p-1) = p+1$ many subgroups, where p^2-1 was the number of non-$(0,0)$ possible g.