Winter 2018, Math 148
Midterm Exam Review

The problems below are intended to help you review for the midterm exam, and may *not* be turned in for credit.

(ER1) True or false: for all $x, y, z \in \mathbb{Z}$ and $n \geq 2$, if $xz \equiv yz \bmod n$, then $x \equiv y \bmod n$.

(ER2) Determine whether $f(x) = x^2 + 1$ divides $g(x) = x^4 + 1$ in $\mathbb{Z}_2[x]$. Does the same hold in $\mathbb{Z}_p[x]$ for some/all of $p > 2$?

(ER3) Is the set

$$R = \{a_d x^d + \cdots + a_1 x + a_0 \mid a_1 = a_2 = a_4 = a_7 = 0\} \subset \mathbb{Q}[x]$$

of polynomials with no terms in degree 1, 2, 4, and 7 a ring? If so, is it a field?

(ER4) Factor $x^4 + 4x^3 + 5x^2 + 2x + 2 \in \mathbb{Z}_7[x]$ as a product of irreducibles.

(ER5) Factor $x^5 + 4x^4 + 3x^3 + 2x^2 + 4x + 2 \in \mathbb{Z}_5[x]$ as a product of irreducibles.

(ER6) Find two distinct irreducible polynomials $f(z), g(z) \in \mathbb{Z}_5[z]$ of degree 3. Show that the product of $z + 1$ and $z^2 + 2z + 1$ is different in the fields $\mathbb{Z}_5[z]/\langle f(z)\rangle$ and $\mathbb{Z}_5[z]/\langle g(z)\rangle$. Why does this not contradict "uniqueness" from the fundamental theorem of finite fields?

(ER7) How many elements of $\mathbb{F}_{27}$ are their own multiplicative inverse? Pick a presentation of $\mathbb{F}_{27}$ (i.e. using an irreducible polynomial over $\mathbb{Z}_3$) and find an element with this property.

(ER8) Factor $x^{16} - x \in \mathbb{Z}_2[x]$ as a product of irreducibles.

(ER9) How many elements of $a \in \mathbb{F}_9$ have a square root (i.e. an element whose square is a)? What about $\mathbb{F}_{16}$?

(ER10) Identify all lines in $\mathbb{F}_3^2$, the 2-dimensional vector space over $\mathbb{F}_3$, that contain $(2, 1)$. You may do this with a picture or by listing the points in each line.

(ER11) Identify 4 parallel lines in $\mathbb{F}_4^2$, the 2-dimensional vector space over $\mathbb{F}_4$. Are there more?

(ER12) Find two mutually orthogonal latin squares of order $n = 7$.