Pries: 405 Number Theory, Spring 2012. Homework 2.

Due: Friday 2/3.

Quadratic rings, polynomials, and modular arithmetic

Read: handout Stillwell 1.8 and Stein section 2.1.

Do 8 of the following problems.

Quadratic rings:

1. Factor 13 in $\mathbb{Z}[i]$.
2. Let $\mathbb{Z}[\sqrt{-13}] = \{a + b\sqrt{-13} \mid a, b \in \mathbb{Z}\}$. Give an example that shows that $\mathbb{Z}[\sqrt{-13}]$ does not have unique factorization.

Polynomials:

Let K be a field (like $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$) and $K[x]$ be the set of polynomials with coefficients in K.

1. Use the Euclidean algorithm to prove: if a polynomial $f(x) \in K[x]$ has a root $\alpha \in K$, then the linear factor $x - \alpha$ divides $f(x)$. Hint: when you divide $a(x) = f(x)$ by $b(x) = x - \alpha$, what can you say about the remainder?
2. If $f(x) \in K[x]$ is a polynomial that factors, and if $\deg(f(x)) \leq 3$, explain why $f(x)$ has a root. Give an example of a field K and a polynomial $f(x) \in K[x]$ with degree 4 that factors but has no root.
3. If $n \mid m$, show that $x^n - 1$ divides $x^m - 1$.

Modular arithmetic:

1. Find all solutions (if any) to the following congruences:
   (a) $7x \equiv 3 \bmod 15$.
   (b) $6x \equiv 5 \bmod 15$.
   (c) $x^2 \equiv 1 \bmod 8$.
   (d) $x^2 \equiv 2 \bmod 7$.
   (e) $x^2 \equiv 3 \bmod 7$.
2. Make a list of the perfect squares in $\mathbb{Z}/7$, $\mathbb{Z}/11$, $\mathbb{Z}/13$. How many are there? Can you explain in general why there are no more or no less?
3. Compute $(p-1)! \bmod p$ for some small primes p, find a pattern and make a conjecture.
4. Compute $(m-1)! \bmod m$ for some small numbers m which are not prime. Find a pattern and make a conjecture. Can you explain why your conjecture is correct?

If you think dogs can't count, try putting three dog biscuits in your pocket and then giving Fido only two of them. - Phil Pastoret