Strange worlds in number theory

In this project, you'll explore worlds where hallowed number facts that you've known since elementary school are no longer always true: for instance, numbers you thought were prime are longer prime; factorizations you thought were unique are no longer unique. As an example, suppose you're working on a difficult problem involving integers that would be dramatically simplified if you could use a number that squared to -5. So you consider the set $\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. In many ways this set behaves like the regular integers $\mathbb{Z}$; for instance, it is a ring. But in exchange for now having an element $\sqrt{-5}$, some surprising things go wrong. For example, 29 is no longer irreducible, since $29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5})$. Neither is 5, since now $5 = -(\sqrt{-5})^2$. On the other hand, 3 still only admits trivial factorizations like $1 \cdot 3$ and $-1 \cdot -3$, and so remains irreducible. How can we predict these differences? We'll be particularly interested in decompositions like $5 = -(\sqrt{-5})^2$, since essentially the prime 5 becomes a square; we call 5 *ramified* in this case. Another shock: unique factorization goes out the window too: $2 \cdot 3$ and $(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ are both distinct ways to write 6 as a product of irreducible elements. Is there any way to fix this? Or at least understand the extent to which things go wrong? It turns out there is, as long as we consider prime ideals instead of prime numbers. There are other new appearances in these strange number-theoretic worlds, and we will get to know them over the course of this project.

The project consists of taking Math 395 (Topics in Algebraic Number Theory) in winter 2014, and then working in groups on further independent projects in spring 2014. The pre-requisite for Math 395 is Math 342 or my permission. The precise nature of your projects will be determined as the course progresses, and according to your interests. Some of the projects may involve doing original mathematics.

Here are some possible topics for the independent projects:

1. **Newton polygons of iterated polynomials**. In this project, you'll learn all about ramification of primes. A great way to understand it comes in the form of the Newton polygon, which you'll learn all about. Particularly vexing is determining so-called wild ramification (sounds fun, doesn't it?), and you'll do some calculations of wild ramification in extensions generated by iterated polynomials. This is a subject that researchers still do not understand well in general, so the door is open to do original work if you notice some patterns that lead to theorems.

2. **Cyclotomic and dynatomic units**. The presence of units other than 1 and -1 in rings like $\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is one of the biggest ruptures with our familiar world of $\mathbb{Q}$. For instance, in $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, the elements $1 + \sqrt{2}$ and $3 - 2\sqrt{2}$ are both units. Gaining a full understanding of these units in general is way too much to hope for, but what about special fields, such as those generated by adjoining to $\mathbb{Q}$ roots of unity? Or those obtained by adjoining roots of an iterated polynomial? You'll read selections from Washington's book *Introduction to cyclotomic fields* and Joe Silverman's book *The arithmetic of dynamical systems* to understand how to generate lots of units in these two cases. As an added bonus, Prof. Silverman will be visiting campus in early spring of 2014.

3. **Number theory in function fields**. There is a surprising analogy between the field $\mathbb{Q}$ of rational numbers and the field $\mathbb{F}_p(t)$ of rational functions with coefficients in the finite field $\mathbb{F}_p$ of p elements. Many of the questions mentioned in the introduction have

natural analogues when we replace $\mathbb{Q}$ by $\mathbb{F}_p(t)$, and sometimes those analogous questions are easier to resolve! You'll explore this connection via reading Michael Rosen's excellent book *Number theory in function fields* and understand how number theory in this context is similar to and different from what we will learn in Math 395.

4. **Extending a result on factorizations of polynomial iterates**. It's an interesting fact that if c is an integer and $c \neq 0$, $c \neq -1$, then every iterate $f^n(x)$ of $f(x) = x^2 + c$ has at most two irreducible factors. If we allow c to be a rational number (again not equal to 0 or -1), then the same is not true, but it is still conjectured that for given c, the number of factors of $f^n(x)$ is bounded independently of n. I and two other authors recently proved this conjecture in the case where c is not the reciprocal of an integer. The reciprocal case – that is, when $c = 1/r$ for some $r \in \mathbb{Z}$ – resisted our method. Yet resolving this case seems within reach, and certainly it should be possible to collect additional computational evidence for the conjecture. Your task is to examine this conjecture as thoroughly as possible and to prove any cases that you can. Understanding what is already known requires using some of the ideas we'll discuss in Math 395.