MATH 788F: THE THEORY OF IRREDUCIBLE POLYNOMIALS

COURSE DESCRIPTION:

The choice of topics will depend on students' interests. Some of the possible topics include Eisenstein's criterion, Newton polygons, irreducibility criteria, finite fields, factoring algorithms, density results, cyclotomic polynomials, other special polynomials, Capelli's theorem, covering problems, Hilbert's irreducibility theorem, sieve methods, and "almost" prime values of polynomials. Some typical results and questions to be considered are:

(1) If $d_n d_{n-1} \dots d_0$ is the decimal representation of a prime, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible (over $\mathbb{Z}$). For example, since my phone number 7776589 is prime,

$$7x^6 + 7x^5 + 7x^4 + 6x^3 + 5x^2 + 8x + 9$$

is irreducible.

(2) If $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) = n$ and there exist $n + 5$ integers m such that $f(m)$ is prime, then $f(x)$ is irreducible.

(3) The probability that a random polynomial in $\mathbb{Z}[x]$ is irreducible over the rationals is 1.

(4) Given any integers $a_1, a_2, \dots, a_{n-1}$, the polynomial

$$\frac{x^n}{n!} + a_{n-1}\frac{x^{n-1}}{(n-1)!} + \cdots + a_2\frac{x^2}{2!} + a_1 x \pm 1$$

is irreducible over the rationals.

(5) Suppose that $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ with $f(x)$ irreducible. When can we conclude that $f(g(x))$ is irreducible?

(6) The polynomial

$$(5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3)x^n + 12$$

is reducible for all $n \geq 0$. What does this have to do with another problem Erdős and Selfridge are willing to pay money for (assuming you come up with the right answer)?

(7) What do we know about prime values of irreducible polynomials? Very little. In particular, if $f(x) = x^2 + 1$, no one has established yet that there are infinitely many integers m for which $f(m)$ is prime? However, in this case, it is known that there are infinitely many integers m for which $f(m)$ has ≤ 2 prime factors. What's known in the general case?