# Comprehensive Exam: Math 788F & 788K

**Definitions/Notation** (for the second part of the test): $\mathbb{N} = \{0, 1, 2, \ldots\}$; $\mathcal{A}$ and $\mathcal{B}$ are subsets of $\mathbb{N}$; $\sigma(\mathcal{A})$ is the Schnirelmann density of $\mathcal{A}$; $\underline{d}(\mathcal{A})$ and $\bar{d}(\mathcal{A})$ are the lower and upper asymptotic densities of $\mathcal{A}$, respectively.

1. Let $n$ and $m$ be integers satisfying $n > m > 0$. Let
$$f(x) = x^n - 738x^m - 9000,$$
and observe that $738 = 2 \times 3^2 \times 41$ and $9000 = 2^3 \times 3^2 \times 5^3$. Prove that $f(x)$ is reducible if and only if $n$ is even and $m = n/2$. In the case that $n$ is even and $m = n/2$, find an explicit factorization of $f(x)$ into irreducibles. (Hint: Even for the latter, it would help to make use of information obtained from Newton polygons of $f(x)$ with respect to primes.)

2. Let $g(x)$ be a non-zero polynomial with integer coefficients.
   (a) Prove that there is an integer $K$ (depending on $g(x)$) such that if $k \geq K$, then every root $\alpha$ of $xg(x) + k$ satisfies $|\alpha| > 1$.
   (b) Prove that there is an integer $P$ (depending on $g(x)$) such that if $p$ is a prime $\geq P$, then $xg(x) + p$ is irreducible over the rationals.
   (c) Prove that there is an integer $P'$ (depending on $g(x)$) such that if $p$ is a prime $\geq P'$, then $xg(x) + 2p$ is irreducible over the rationals.
   (d) Fix integers $a$ and $d$ with $d \neq 0$. Prove that there is an integer $N = N(a, d, g(x))$ such that if $p$ is a prime $\geq N$, then $(x - a)g(x) + dp$ is irreducible over the rationals.

3. (a) Let $f_1(x)$, $f_2(x)$ and $g(x)$ be polynomials with complex coefficients. Prove that $R(f_1f_2, g) = R(f_1, g)R(f_2, g)$.
   (b) Let $f(x)$, $g_1(x)$ and $g_2(x)$ be polynomials with complex coefficients. Prove that $R(f, g_1g_2) = R(f, g_1)R(f, g_2)$.
   (c) Let $f(x)$ and $g(x)$ be polynomials with complex coefficients and of degrees $n$ and $r$, respectively. Prove that $R(f, g) = (-1)^{nr}R(g, f)$.
   (d) Let $f(x)$, $g(x)$ and $h(x)$ be polynomials with complex coefficients with $f(x) = g(x)h(x)$. Prove that $R(f, f') = R(g, h)R(h, g)R(g, g')R(h, h')$.
   (e) Let $f(x) = g(x)h(x)$ where $g(x) = x^2 + ax + b$ and $h(x) = x + c$ (with $a$, $b$, and $c$ complex numbers). Prove that $R(f, f') = -(a^2 - 4b)R(g, h)^2$.
   (f) Let $a$ and $b$ be integers. Prove that if $a^2 - 4b$ is a square modulo an odd prime $p$, then $x^2 + ax + b$ is reducible modulo $p$.
   (g) Let $f(x) = x^3 - x^2 - 2x + 1$. Show that $R(f, f') = -49$.
   (h) Let $f(x) = x^3 - x^2 - 2x + 1$, and let $p$ be a prime. Using the information just obtained, explain why $f(x)$ cannot factor as a product of exactly two irreducible polynomials (one of degree 2 and one of degree 1) modulo $p$.

4. (a) For which primes $p$ does the cyclotomic polynomial $\Phi_7(x)$ have a root modulo $p$?
   (b) For which primes $p$ does $\Phi_7(x)$ have an irreducible quadratic factor modulo $p$?
   (c) Let $p$ be a prime. Suppose $a$, $b$, and $c$ are integers satisfying

$$a+b+c \equiv 1 \pmod{p}, \quad ab+ac+bc \equiv -2 \pmod{p}, \quad \text{and} \quad abc \equiv -1 \pmod{p}.$$

   Prove that

$$\Phi_7(x) \equiv (x^2+ax+1)(x^2+bx+1)(x^2+cx+1) \pmod{p},$$

   where the quadratic factors shown are not necessarily irreducible.
   (d) Let $f(x) = x^3 - x^2 - 2x + 1$. Recall the conclusion of part (h) of the previous problem. Deduce from the previous parts of this problem that if $f(m)$ is divisible by a prime $p$ different from 7, then $p \equiv \pm 1 \pmod{7}$.
   (e) Deduce from the above that there exist infinitely many primes $\equiv -1 \pmod{7}$.

5. (a) Let $\mathcal{A} = \bigcup_{k=0}^{\infty} \{2^{2k}, 2^{2k}+1, \ldots, 2^{2k+1}-1\} = \{1, 4, 5, 6, 7, 16, \ldots, 31, 64, \ldots, 127, \ldots\}$.
   Find $\sigma(\mathcal{A}) = \_\_\_\_$ ; $\underline{d}(\mathcal{A}) = \_\_\_\_$ ; $\bar{d}(\mathcal{A}) = \_\_\_\_$.
   (b) Suppose $\mathcal{A}$ is the set of **positive** cubes, and $\mathcal{B}$ is a set of **positive** integers so that $\mathcal{A} + \mathcal{B}$ contains all integers $\geq 2$. Let $B(n) = \#\{b \in \mathcal{B} : b \leq n\}$. Prove that $B(n) \geq n^{2/3}$ for all $n \geq 1$.

6. (a) State the Cauchy-Davenport-Chowla theorem.
   (b) Prove that for every **odd** prime $p$ and $0 \leq m \leq p-1$, there are integers $x_1, x_2, x_3$ such that $x_1^3 + x_2^3 + x_3^3 \equiv m \pmod{p}$. Use the Cauchy-Davenport-Chowla Theorem, plus the fact that the set $\{x^k \mod p : 1 \leq x \leq p-1\}$ has cardinality $\frac{p-1}{(k,p-1)}$ for odd primes $p$. Note that some of the $x_i$ may be divisible by $p$.

7. The main sieve result proved in class (Theorem 18) is the following:

**Theorem.** Suppose $\mathcal{A}$ is a finite set of positive integers, $\omega$ is a multiplicative function satisfying $\omega(p) < p$ for primes $p$, and for some real numbers $\kappa$ and $A$,

$$\prod_{y_1 \leq p < y_2} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \leq \left(\frac{\log y_2}{\log y_1}\right)^{\kappa} \exp(A/\log y_1), \quad (2 \leq y_1 \leq y_2). \tag{1}$$

Suppose $\mathcal{P}$ is a set of primes $\leq X^{1/8}$, $P = \prod_{p \in \mathcal{P}} p$ and $r_d = |\mathcal{A}_d| - \frac{\omega(d)}{d} X$ with $|r(d)| \leq \omega(d)$ for $d|P$. Then, for large $X$,

$$S(\mathcal{A}, \mathcal{P}) \leq e^{e^{\kappa}} X \prod_{p \in \mathcal{P}} \left(1 - \frac{\omega(p)}{p}\right).$$

Use this theorem to prove that the number of primes $p \leq x$ for which $p+6$ is prime, is $O(x/\log^2 x)$. Be sure to state what $\omega(d)$ is, what $\mathcal{P}$ is, and to prove (1).

8. Let $\omega(n)$ be the number of distinct prime factors of $n$ and let $\Omega(n)$ be the number of prime factors counted with multiplicity. Let $\tau_k(n)$ be the divisor function that counts the number of un-ordered $(d_1, d_2, \cdots, d_k)$ with $n = d_1 d_2 \cdots d_k$. For $n = p_1^{e_1} \cdots p_r^{e_r}$, we have

$$\tau_k(n) = \binom{e_1 + k - 1}{e_1} \cdots \binom{e_r + k - 1}{e_r}.$$

A theorem of Hardy and Ramanujan states that for every $\varepsilon > 0$,

$$\#\{n \le x : |\omega(n) - \log\log x| > \varepsilon \log\log x \text{ or } |\Omega(n) - \log\log x| > \varepsilon \log\log x\} = o(x).$$

Use this result to prove that for every $\varepsilon > 0$,

$$\#\{n \le x : k^{(1-\varepsilon)\log\log n} \le \tau_k(n) \le k^{(1+\varepsilon)\log\log n}\} = x - o(x);$$

i.e., $\tau_k(n) = k^{(1+o(1))\log\log n}$ for most $n$. Hint: first prove that $k \le \binom{e+k-1}{e} \le k^e$ for $e \ge 1$, and use this to show $k^{\omega(n)} \le \tau_k(n) \le k^{\Omega(n)}$.