MATH 145 Extra Questions

Patrick Ingram

This set of questions is supposed to give you some idea of what sorts of things to expect on the final exam. The number of questions below does not reflect the length of the actual final exam (this list would take anyone more than 2.5 hours). You should also include the assignments and midterm in your list of questions to look at, as well as the exercises in the sections of the notes that we covered. The emphasis in this set of problems is biased a little more towards the end of the course, since the assignments and midterm covered earlier material. The final exam will be comprehensive, covering the entire course.

Some general tips on studying for finals: it's usually a good idea to spread your studying out over time. It's not possible, for most people, to concentrate on one topic for several hours at a time, so the only way to really effectively review things is to do a small amount of studying every day. This also gives you the option of studying one subject as a break from studying others. Of course, it's also important to take *real* breaks. In preparing for the final exam, it is beneficial for you to attempt these problems in an exam-like setting (i.e., without looking things up, or consulting other people). It's easy to convince yourself that you know how to do something when someone else explains it, but this is not a good indicator of how you'll do on the final.

Problem 1. i. Compute $\gcd(156400, 89148)$, and find integers x, y such that

$$156400x + 89148y = \gcd(156400, 89148).$$

ii. Compute $g(x) = \gcd(x^4 - 2x^3 - 5x^2 + 4x + 6, x^4 - 3x^3 + 3x^2 + 6x - 10)$, and find polynomials $s(x), t(x) \in \mathbb{Q}[x]$ such that

$$(x^4 - 2x^3 - 5x^2 + 4x + 6)s(x) + (x^4 - 3x^3 + 3x^2 + 6x - 10)t(x) = g(x).$$

Problem 2. Prove the Chinese Remainder Theorem for polynomials. That is, if F is a field, and $f(x), g(x) \in F[x]$ satisfy $\gcd(f(x), g(x)) = 1$, prove that for any $a_1(x), a_2(x) \in F[x]$ there is a $b(x) \in F[x]$ such that

$$\left\{ \begin{array}{l} s(x) \equiv a_1(x) \pmod{f} \\ s(x) \equiv a_2(x) \pmod{g} \end{array} \right\}$$

if and only if

$$s(x) \equiv b(x) \pmod{fg}.$$

Furthermore, prove that $b(x)$ is unique modulo fg.

Problem 3. Compute the least non-negative residue of

i. $7^{2222} \pmod{11}$.

ii. $5^{2010} \pmod{4321}$.

iii. $n^{4n+8} + n^2 - 1 \pmod{5}$ (your answer will be in the form of a congruence condition on n).

Problem 4. Explain how the RSA cryptosystem works, in as much detail as possible. Explain, in particular, why it is secure (or, at least, thought to be secure).

Problem 5. Let F be a field, let $f(x) \in F[x]$ be a polynomial, and consider the commutative ring $F[x]/(f)$. Prove that for any $[g] \in F[x]/(f)$, $[g]$ is a unit (has a multiplicative inverse) if and only if $\gcd(f(x), g(x)) = 1$.

Problem 6. The Lucas numbers L_n are defined by $L_0 = 2$, $L_1 = 1$, and

$$L_n = L_{n-1} + L_{n-2}.$$

i. If $\tau = (1 + \sqrt{5})/2$ is the golden ratio, prove that

$$L_n = \tau^n + (-\tau)^{-n}$$

for all n (it might be useful to note that $\tau^2 - \tau - 1 = 0$).

ii. Recall that the Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$, and

$$F_n = F_{n-1} + F_{n-2}.$$

Prove that, for all n, $L_n = F_{n+1} + F_{n-1}$.

iii. Prove that

$$F_n = \frac{\tau^n - (-\tau)^{-n}}{\sqrt{5}}.$$

iv. Prove that $L_n^2 - 5F_n^2 = 4(-1)^n$, for all n, and calculate the limit

$$\lim_{n \to \infty} \frac{L_n}{F_n}.$$

Problem 7. Let $a, b \in \mathbb{Z}$ be positive integers, with $\gcd(a, b) = 1$. We know that, for any $n \in \mathbb{Z}$, there is a solution $x, y \in \mathbb{Z}$ to $ax + by = n$. Prove that if $n \geq (a-1)(b-1)$, then there is a solution with $x, y \geq 0$.

Problem 8. Find a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\sqrt{5}+\sqrt{6}) = 0$. Show that this polynomial is irreducible.

Problem 9. Suppose that $m \in \mathbb{Z}$ is a product of exactly two distinct prime numbers, that $m = 20717933$, and that $\varphi(m) = 20706588$. Find m.

Problem 10. Let $a \in \mathbb{C}$ be a root of some irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree at least two. Show that a is not a rational number. Give as much detail as possible.

Problem 11. The commutative ring $\mathbb{Z}_3[x]/(x^2-1)$ has 9 elements. Write out a multiplication and addition table for this ring. Is $\mathbb{Z}_3[x]/(x^2-1)$ a field?

Problem 12. Recall that $\sigma(n) = \sum_{d|n} d$ is the sum of the divisors of n.

i. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where the p_i are distinct prime numbers, and $e_i \geq 1$, give a formula (in terms of the p_i and e_i) for $\sigma(n)$. Give a full justification for your formula (you may assume that σ is a multiplicative function).

ii. If p and q are distinct primes with $pq = 150947$ and $\sigma(pq) = 151776$, find p and q.

Problem 13. i. Prove that if $n \in \mathbb{Z}$ satisfies $n \equiv 5 \pmod 6$, then there is a prime $p \mid n$ with $p \equiv 5 \pmod 6$.

ii. Prove that there are infinitely many primes $p \equiv 5 \pmod 6$.

Problem 14. Find the remainder when $2^{17^{15^{13}}}$ is divided by 13.

Problem 15. Let $a_1, a_2, ...$ be a sequence of positive integers such that

$$a_m \mid a_{m+1}$$

$$\sum_{i=m+1}^{\infty} \frac{1}{a_i} < \frac{1}{a_m}$$

and

$$a_{m+1} > a_m^m$$

for all $m \geq 1$. Prove that $\sum_{m=1}^{\infty} \frac{1}{a_m}$ is a transcendental number.

Problem 16. Construct a field with 4 elements. Write down the addition and multiplication table for this field.

Problem 17. i. Let F be a field, and let $f(x), g(x) \in F[x]$. Prove that if $f(a) = 0$ and $g(a) = 0$, and $h(x) = \gcd(f(x), g(x))$, then $h(a) = 0$.

ii. Prove that if $f(x) \in \mathbb{Q}[x]$ has a root in $\mathbb{R}$ which is also a critical point (so $f(a) = f'(a) = 0$ for some real number a), then $f(x)$ is not irreducible in $\mathbb{Q}[x]$. (Note: the root might not be in $\mathbb{Q}$!)

Problem 18. Find all solutions to

$$x^2 + 13 \equiv 56 \pmod{221}$$

(your answer should be in the form of congruence classes modulo 221).

Problem 19. Show that the following polynomials are irreducible in $\mathbb{Z}[x]$.

i. $x^4 + 3x^3 - 27x^2 + 15x + 21$

ii. $x^3 + x^2 - 2x + 7$

iii. $x^4 + x^3 + x^2 + x + 1$ (hint: let $x = y + 1$)

Problem 20. Let p be a prime.

i. Show that the only elements of $\mathbb{Z}_p$ which are their own multiplicative inverses are 1 and -1.

ii. Prove Wilson's Theorem, that

$$(p-1)! \equiv -1 \pmod{p}.$$

iii. Let F be a finite field. State and prove a generalization of Wilson's Theorem for F. (That is, write down some fact about F which is the same as the congruence above if $F = \mathbb{Z}_p$, and then prove that fact for all finite fields.)

Problem 21. The Mersenne sequence is the sequence of integers $M_n = 2^n - 1$.

i. Prove that $k \mid n$ implies $M_k \mid M_n$.

ii. Prove that if M_n is prime, then n is prime.

iii. Show that the converse of part ii is not true (so, part ii is not an "if and only if").

iv. For a prime p, define a function v_p on the positive integers such that $v_p(n)$ is the largest $e \geq 0$ such that $p^e \mid n$ (in other words, if $n = p^e m$, where $p \nmid m$, then $v_p(n) = e$). Show that

$$v_p(ab) = v_p(a) + v_p(b)$$

and

$$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}.$$

v. Show that if $p \mid M_n$, then for any integer $m \geq 1$, $\gcd(m, p) = 1$ if and only if

$$v_p(M_{mn}) = v_p(M_n).$$

Problem 22. i. Show that every integer of the form

$$2n^{18} - 10n^{12} + n^6 + 7$$

is composite, for $n \geq 1$.

ii. Show that every integer of the form

$$n^3 + n^2 + 4$$

is composite, for $n \geq 1$.

Problem 23. Suppose that you have a certain number of apples. When you try to divide them among 7 people, and you give them each an equal number, there are 5 left over. One of the people leaves (without taking any apples), and you try again to divide them out equally. This time there are 2 left over. Finally, one more person leaves (without taking any apples) and you try again. This time there are 4 left over. What is the smallest (positive) number of apples which makes this scenario possible?