MATH 328 (Rusin) — FINAL EXAM ANSWERS

I can't resist one last "teachable moment" for this Number Theory class!

1. What is the largest power of 12 that divides $18^{24} + 24^{18}$?

ANSWER: This is your token Fundamental Theorem of Arithmetic question: we can decide whether $A|B$ or not by looking at the prime factors of A and B. In this case, $A = 2^{2k}3^k$ for some k, and $B = 2^{24}3^{18}(2^{30} + 3^{30})$, where the factor in parentheses is coprime to both 2 and 3. Hence $A|B$ iff $2k \le 24$ and $k \le 18$, which is to say, iff $k \le 12$.

2. The *Tribonacci numbers* T_n are defined by $T_1 = 0, T_2 = 0, T_3 = 1$. and for $n > 3$ by $T_n = T_{n-1} + T_{n-2} + T_{n-3}$. Show that for all $n > 0$ we have $T_n \le 2^{n-3}$.

ANSWER: And this is your token Proof By Induction question. The statement $P(n)$: "$T_n \le 2^{n-3}$" is obviously true for $n = 1, 2, 3$. Let me phrase this for once in terms of a "minimal criminial": if the set S of "criminals", positive integers n for which $P(n)$ is false, isn't empty, then S has a least element n (which is now obviously at least 4). Then $n-1, n-2$ and $n-3$ are positive integers for which $P(n)$ is true, and so we know

$$T_{n-1} \le 2^{n-4}, \qquad T_{n-2} \le 2^{n-5}, \qquad T_{n-3} \le 2^{n-6}$$

Add these, and factor out 2^{n-6}, to get $T_n = T_{n-1} + T_{n-2} + T_{n-3} \le 2^{n-6}(4 + 2 + 1) < 2^{n-6}(8) = 2^{n-3}$ which shows that in fact this n is not a criminal, after all. Thus S is empty: the statement $P(n)$ is true for all natural numbers n.

3. (a) Prove that for every $n > 0$, the sum of the first n even natural numbers is $n^2 + n$.

(b) The number $a = 41$ has the following remarkable property. First of all, this a is prime. If we add 2 to a, we get another prime (43). If we add 4 to this, we get another prime (47). Continue in this way, each time adding the next even number. Every single one of the numbers attained in this way is prime until the composite 40th term ($1681 = 41^2$)

Prove that no matter which number $a > 0$ is used for the start of this sequence, we will always eventually encounter a composite number.

ANSWER: Part (a) is well known. Many of you proved it by induction, which is fine. But consider the sum

$$S = 1 + 2 + \ldots + (n-1) + n$$
$$\text{i.e. } S = n + (n-1) + \cdots + 2 + 1$$

of the first n integers. Adding the right sides together clearly shows that the sum of the first n even integers will then be $2S$. But we may add the two right-hand sides vertically; there are n pairs that each sum to $n + 1$, so we have $2S = n(n + 1)$.

From (a) we then conclude that the nth term in the sequence in (b) will be $a+(n^2+n)$. In particular the $(a-1)$st term of the sequence is $a + (a-1)^2 + (a-1) = a^2$ which is obviously composite (unless $a = 1$; for that value of a, the composite number 21 is the fifth term in our sequence).

This exercise suggests a host of questions!

It's actually quite rare for many terms of the sequence $a+n+n^2$ to be prime. Just to have both a and $a+2$ be prime means they are "twin primes"; it is widely expected that there are infinitely many of these but no one has a proof. In order to have $a, a+2$, and $a+6$ all prime is not particularly rare, but asking that the first four or five terms in the sequence all be prime makes for a sparser and sparser set. The list of integers for which the initial ten terms are all prime begins 11, 17, and 41, but then the next two terms are 844427 and 51448361. And only $a = 17$ and $1 = 41$ have more than ten initial primes, until $a = 180078317$ (which has only eleven). The next case with 12 primes is $a = 1761702947$, the next with 13 is $a = 8776320587$, the next with 14 is $a = 27649987598537$, and the next with 15 is $a = 291598227841757$. After $a = 41$, the second-place winner for the longest known sequence of initial primes is $a = 234505015943235329417$, which comes in with a paltry 21 initial primes. (And yet: it is conjectured that there are infinitely many primes with any prescribed number of initial primes in the sequence!)

So the fact that ALL the first 40 terms are prime when $a = 41$ is quite amazing (an oddity noticed by Euler). In fact $a = 41$ is proved to be the largest prime for which all $a-1$ initial terms are prime. This piece of information is related to some fantastic properties of the number $163 = 4 \cdot 41 - 1$, such as the observation that $e^{\pi\sqrt{163}}$ is so close to an integer! This is some heavy-duty number theory ...

We need not look only at $f(n) = a + n + n^2$. If $f(n)$ is any polynomial with integer coefficients, then let a be its constant term. It is then clear that $f(ka)$ is a multiple of a for each integer k. This multiple might, for some integers k, be a itself, or $-a$, or 0; but a polynomial of degree $d > 0$ can only attain any particular value at most d times, so in particular $f(ka)$ must be a *composite* multiple of a for all but a finite number of integers k, as long as $|a| > 1$.

Even if a polynomial has a constant term equal to 0 or ± 1, it must attain composite values infinitely often. Indeed, we must have $|f(n)| > 1$ for all but a finite number (at most $3d$) of integers n; if a is a larger-magnitude value that f assumes at some integer n_0 then $g(n) := f(n + n_0)$ is a polynomial whose value at 0 — that is, whose constant term — is a and so the previous paragraph applies: g, and thus f, attains composite values infinitely often.

So there is no polynomial whose values are all primes. How about asking for at least *infinitely many* prime values? This is harder. The polynomial $f(n) = 4n - 1$ takes on a prime value infinitely many times; a proof is in your book. In fact as long as $\gcd(a, b) = 1$, the same is true of $f(n) = an + b$; that's a difficult theorem by Dirichlet. For polynomials of higher degree, little is known. We don't even know if $f(n) = n^2 + 1$ takes on infinitely many prime values.

These are polynomials of one variable. Interestingly, there *is* a polynomial of 26 variables whose *positive* values are precisely the set of all primes! This is due to the work of Matiyasevich as part of his proof that there can be no algorithm which decides whether or not a Diophantine problem has solutions. (In other words, no machine can be expected to reliably answer all the questions that look like my Problem 6, below.)

4. Show that if a and b are two coprime integers, then no odd prime p can divide both $a + b$ and $a^2 + b^2$.

ANSWER: If $p|(a+b)$ then $p|(a+b)^2 = (a^2+b^2)+2ab$. So if we also know $p|(a^2+b^2)$, then $p|2ab$. Since p is odd, this means $p|ab$. Now use Euclid's characterization of primes to see that p must divide a or b — or both, and indeed since $p|(a+b)$, if p divides one of these, it *must* divide the other too. But that would contradict the fact that a and b were given to be coprime.

You could also phrase this with arithmetic mod p: if $a+b \equiv 0$ then $a \equiv -b$ so $a^2 \equiv b^2$. But if $a^2+b^2 \equiv 0$ then this means $2a^2 \equiv 0$. Since 2 is invertible mod p, we get $a \cdot a \equiv 0$. But since we are working modulo a prime, the product of two nonzero congruence classes would be nonzero; thus we must in fact have $a \equiv 0$, in which case $b \equiv 0$ too, again contradicting coprimality. Same proof, really, just different language.

Incidentally, if a and b are coprime and both odd, then the not-odd prime 2 divides both $a+b$ and a^2+b^2. But the latter would be congruent to 2 mod 4, so even in this case we find the gcd of $a+b$ and a^2+b^2 can be no larger than 2.

5. Show that if a is any integer coprime to 561, then $a^{560} \equiv 1 \pmod{561}$.

ANSWER: You cannot simply quote Fermat's Theorem because 561 is not prime! In fact it factors as $561 = 3 \cdot 11 \cdot 17$, so actually what we must show is that if a is not divisible by 3 nor 11 nor 17, then $a^{560}-1$ is divisible by 3 and by 11 and by 17.

But each of these conclusions *does* follow from Fermat's theorem, since 560 is a multiple of $p-1 = 2$ or $= 10$ or $= 16$.

This question is really just testing your grasp of the Chinese Remainder Theorem, but it is useful because it shows that the "Fermat Test" for primality can yield a false positive. That is, if you test integers a at random to see whether $a^n \equiv a \bmod n$, then if we ever get a negative answer we know a is definitely composite, while if we get a positive answer for every integer a, we don't know n is really prime; n might be a "pseudo prime" like 561. It turns out these impostors are rarer than the primes themselves, and there are ways to sniff them out, but they do make primality testing into a probabilistic exercise.

(The usual way to detect a pseudo-prime is yes, to check that $a^{n-1} \equiv 1$ for some randomly-selected values of a, but then also to look at the whole sequence

$$a^{(n-2)}, a^{(n-1)/2}, a^{(n-1)/4}, a^{(n-1)/8}, \ldots$$

for as many powers of two in the exponent as we can get; each one of the terms in the sequence should be the square of its successor, and the first term is a 1. If there is ever a 1 which is not followed by either a 1 or a -1, then n is not prime, because modulo a prime there are only these two square roots of 1. Conversely, if n is not prime then for at least half of the values of a, we will have a 1 that is not followed by ± 1. So the probability that k random choices of a will not reveal a composite number is at most $1/2^k$. Running a small number of such tests gives great confidence that a number really is prime.)

6. Find all integer solutions (x, y) to *one* of the following equations

$$(a)\ 4x+9y=35 \qquad (b)\ 6x^2+xy-12y^2=35 \qquad (c)\ 3x^2-y^2=35$$

For extra credit, find all integer solutions to either or both of the other equations.

ANSWER: For (a), write the equation as $4(x-2) = 9(3-y)$; since 4 divides the left side of this equation, it divides the right side; since 4 and 9 are coprime, that means $4|(3-y)$, i.e. $y = 3-4u$ for some integer u. Substitute into $4(x-2) = 9(3-y)$ to then see $x = 2+9u$. That is, the general solution is $(x, y) = (2, 3) + u(9, -4)$. (In particular, there do exist solution pairs, in fact infinitely many of them.

For (b), factor the left side to get $(2x+3y)(3x-4y) = 35$, which requires $2x+3y$ and $3x-4y$ to be a complementary pair of divisors of 35, that is, they equal respectively d and $35/d$ where d is one of the elements of $\{\pm 1, \pm 5, \pm 7, \pm 35\}$. In each case we get a pair of linear equations to solve for x and y. Solve in each case and you will discover the solution pair (x, y) is not integral, that is, there are no integer solutions to the original problem.

I will confess I screwed up as I prepared the problem; I thought I had arranged the coefficients so that at this point I would be solving the equations $2x+3y = d, 3x+4y = 35/d$, which in fact has an integer solution pair (x, y) for each of the 8 values of d. (I will let you work them out but since I lost a minus sign by this point, what you are actually computing are the solutions to $6x^2 + 17xy + 12y^2 = 35$.) The point of this example was simply to show that there could be a Diophantine polynomial problem that had a non-zero but finite solution set — different from (6a) and different from (6c).

For part (c), there are no solutions in integers. If $p = 5$ or $p = 7$ then the congruence $3x^2 - y^2 \equiv 35 \bmod p$ has only the trivial solution $x \equiv y \equiv 0$. Indeed for each of these primes 3 is not a quadratic residue, so we would have a contradiction from the equation $3 \equiv (x^{-1}y)^2$ unless x is not invertible, i.e. $x \equiv 0$, which in turn forces $y^2 \equiv 0$ hence $y \equiv 0$. But even for the trivial solution mod p we encounter a restriction: if $x = pX$ and $y = pY$ then we would have $p^2(3X^2 - Y^2) = 35$, which is a contradiction since p^2 does not divide 35. So there can be no such integers X and Y, hence no solutions (x, y).

For comparison, there are infinitely many solutions to the equation $3x^2 - y^2 = 44$, and more generally we can have infinitely many solutions to a quadratic Diophantine equation, if we don't have a mod-p restriction.

The Hasse-Minkowski theorem applies here. What that theorem says is *almost* the following statement: given a single quadratic Diophantine equation in multiple variables, we count the number N of primes p modulo which our equation has no solution modulo p. Then (a) if $N > 0$ then there is no solution in integers, (b) if $N = 0$ then there is a solution in integers, and (c) N is even . Part (a) is trivial, the others are not. (To make this statement correct, you must first raise N by 1 if there is no solution in real numbers. Moreover, a prime should really be included in the count N when there is no solution in *the ring of p-adic numbers*. I will leave you to look that up.)

7. Show that if $x \equiv 4 \pmod 9$ or $x \equiv 5 \pmod 9$ then it is impossible to write x as a sum of three perfect cubes (positive, negative, or zero).

ANSWER: This was a chance for you to recycle the ideas from the second midterm. Every integer is either a multiple of 3 or one off from a multiple of 3; hence the cubes mod 9 are $(3x)^3 \equiv 0$ and $(3x \pm 1)^3 \equiv \pm 1$. It follows that any number which is a sum of three cubes is congruent (modulo 9) to an integer whose absolute value is at most 1. So any sum of 3 of these is congruent to an integer of absolute value at most 3, i.e. to one of $-3, -2, -1, 0, 1, 2, 3$ But any integer congruent to 4 or 5 mod 9 is congruent to none of

these.

At that point one might wonder whether every integer that is congruent to one of the seven "allowed" residues mod 9 is actually a sum of three cubes. The answer is: we don't know. It was only last Fall that a solution was found for the (famous!) number 42:

$$(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42.$$

The case n=114 is still open, if you'd like to give is a whirl ...

8. Use Quadratic Reciprocity to determine whether or not 73 is a square modulo 59.

ANSWER: This is a sraightforward use of our theorems to evaluate Legendre symbols. We have

$$\left(\frac{73}{59}\right) = \left(\frac{14}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{7}{59}\right) = (-1)^{(59^2-1)/8} \cdot - \left(\frac{59}{7}\right) = + \left(\frac{3}{7}\right) = - \left(\frac{7}{3}\right) = - \left(\frac{1}{3}\right)$$

which is -1, so no, 73 is not a square mod 59.

Many of you noted that $\left(\frac{73}{59}\right) = \left(\frac{59}{73}\right)$ which is true, but I didn't ask about the latter and you never used it, so I don't know why you mentioned it!

9. Is 16 a cube modulo $p_1 = 2000387$? I will tell you that p_1 is prime and 2 is a primitive root modulo p_1; that may help. Answer the same question with the prime modulus $p_2 = 6001747$. for which 2 is again a primitive root.

ANSWER: I claim 16 is a cube modulo p_1 but is not a cube modulo p_2. The difference is simply because $p-1$ is not a multiple of 3 in the first case, but is a multiple of 3 in the second case.

So suppose p is any prime with $p \equiv 2 \bmod 3$, say $p = 3k+2$. Then every element of $\mathbf{Z}_p$ is a cube. Indeed, $p+(p-1) = 3(2k-1)$ is a multiple of 3, so with the help of Fermat's theorem we may compute

$$a = a \cdot 1 \equiv a^p \cdot a^{p-1} = a^{p+(p-1)} = (a^{2k-1})^3$$

so that a is a cube mod p.

In the other case, suppose p is any prime with $p \equiv 1 \bmod 3$. Then only 1/3 of the congruence classes mod p are cubes, specifically, those whose indices (base r, where r is any primitive root) are multiples of 3 (modulo $\phi(p) = p-1$). In our case the index of 16 (using $r = 2$) is clearly 4, and that's not a multiple of 3. Indeed, we may compute $\mathrm{ord}(2^4) = \mathrm{ord}(2)/\gcd(4, \mathrm{ord}(2))$ but since 2 is a primitive root its order is $p-1 = 6001746$, which is even but not a multiple of 4. Thus $\mathrm{ord}(16) = 3000873$, whereas every cube has an order less than $p/3$. Another approach: if $x^3 \equiv 16 = 2 \cdot 8$, then $2 \equiv (2^{-1}x)^3 \bmod p$, which means the order of 2 wouuld be at most $(p-1)/3$, contradicting the statement that 2 is a primitive root.

There are multiple ways to express these same ideas; for example, you could try to solve $x^3 \equiv 16$ by writing $x = 2^k$ for some k (which is possible because that's the whole point of primitive roots!) and then seeing what values of k might make $x^3 = 2^4$. Answers varied but overall students did well with this hard question.

10. If we should be forced to hold our Fall 2020 classes online, how should we do it? What worked this semester — in our class or any other class you took — and what did not work?