189-346B/377B: Number Theory

Midterm Exam: Corrections

Friday, February 11

General remarks: Each question in the midterm was graded out of 20, for a maximum possible score of 100. So that you know where you stand with respect to the rest of the class, here is the grade distribution in each section.

Grade	Math 346	Math 377
0-19	1	0
20-24	1	0
25-29	2	0
30-44	1	1
45-49	1	0
50-54	2	0
55-59	4	1
60-64	4	3
65-69	6	0
70-80	2	7
81-85	1	4
90-94	0	3
95-100	0	2

I thought that the grades were somewhat lower than I expected. Do go over the solutions below carefully to find out where you went wrong and learn from your mistakes.

1. Show that the gcd of two integers a and b is a linear combination of a and b, i.e., that if $d = \gcd(a, b)$ then there exist integers m and n for which

$$d = ma + nb.$$

Solution: This is a proof that was done in class. The solution I prefer is to let L be the set of all *strictly positive* linear combinations of a and b, and to let $d = ma + nb$ be the *least element* in this set. The remainder after the division of a by d is strictly less than d, and is *also* a linear combination of a and b. Hence, it must be 0, by the minimality of d. Therefore d divides a, and, by the same argument, it also divides b. It follows that d is a common divisor of a and b. It is also the greatest such, since any integer that divides both a and b must necesarily divide anything in L. Hence d is the *gcd* of a and b, and, by its very construction, it is a linear combination of these two integers.

A second solution, which I like less because it is less elegant, but still gave full credit for, was to describe the Euclidean algorithm for calculating the gcd of a and b and observe that this algorithm also leads to an expression for the gcd as a linear combination of a and b.

2. State two number-theoretic problems that are believed to be computationally intractable, and for each problem, name a cryptosystem that exploits this presumed intractability. (This question is just to test your knowledge of the salient points in the material covered in class. You do not need to provide descriptions of the cryptosystems in question, only their names. If you can't remember the names, then a brief description will do...)

Solution. Almost everyone got this question right. The two problems are

1. The problem of finding the prime factors p and q of an integer $n = pq$ when these factors are of size roughly 2^{512}. The RSA public-key cryptosystem is based on the presumed intractability of this factoring problem.

2. The problem of computing the discrete logarithm in $(\mathbf{Z}/p\mathbf{Z})^\times$, for a large prime p of size roughly 2^{512}. The Diffie-Hellman key exchange protocol exploits the presumed intractability of this problem. Or, somewhat more precisely, the presumed intractability of the so-called *Diffie-Hellman problem*, which is to *efficiently* calculate g^{ab} mod p given the knowledge of p, g, g^a and g^b.

3. Compute

$$7^{403275023750023740523040602} \pmod{101}.$$

You should express your answer as an integer between 0 and 100.

Solutions. The modulus 101 is prime and 7 is of course nonzero modulo 101. Therefore, by Fermat's little theorem,

$$7^{100} \equiv 1 \pmod{101},$$

and, more generally, if $e = 100 \cdot q + r$ is any integer, with r its least residue modulo 100, then

$$7^e = 7^{100 \cdot q + r} = (7^{100})^q \times 7^r = 1^q \times 7^r = 7^r \pmod{101}.$$

So least residue of 7 to that horrible exponent above is just

$$7^2 = 49 \pmod{101}.$$

A useful hint in this question was the sheer size of the exponent, combined with the knowledge that your instructor is basically kind and well-meaning, and hence would not saddle you with a huge calculation in a one-hour exam! So the solution had to be something computationally simple; in this case, only the last two digits of the exponent mattered in the problem.

4. A *Sophie Germain prime* is a prime p of the form $1 + 2q$ where q is also a prime. Assume that p is such a prime. Show that $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ is a primitive root modulo p if and only if

$$a \neq \pm 1, \quad a \neq b^2 \pmod{p}, \text{ for any } b \in (\mathbf{Z}/p\mathbf{Z})^\times.$$

Find the smallest primitive root modulo 23.

Solution. For the first part, note that the order of an element $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ necessarily divides $\varphi(p) = p - 1 = 2q$. Since q is prime, this order must therefore be either 1, 2, q or $2q$. But it is clear that

$$\text{order}(a) = \begin{cases} 1 & \text{iff } a = 1; \\ 2 & \text{iff } a = -1; \\ q & \text{iff } a \neq \pm 1 \text{ and } a^q = a^{(p-1)/2} = 1; \\ 2q & \text{otherwise.} \end{cases}$$

But by Euler's criterion, $a^{(p-1)/2} = 1 \pmod{p}$ if and only if a is a square mod p, and the result follows.

For the second part of the question, you could observe that 2 is not a primitive root modulo 23 because

$$2 \equiv 25 = 5^2 \pmod{23} \tag{1}$$

and hence, (since 23 is a Sophie Germain prime) the order of 2 is 11. Likewise, we observe that

$$3^3 = 27 \equiv 4 \equiv 2^2 \pmod{23},$$

and therefore 3 is also a quadratic residue modulo 23. On the other hand, 5 *is* a primitive root since its order is equal to 22 by equation (1).

5. Solve the equation

$$x^2 + 1 = 0 \pmod{101^2}.$$

Solution: Any root modulo 101^2 is necessarily a root modulo 101. Since 101 is prime, there are at most two roots modulo 101, which can easily be found by inspection: they are $s_1 = 10$ and $s_2 = -10$. We then note that, after setting $f(x) = x^2 + 1$,

$$f'(s_1) = 20 \neq 0 \pmod{101}, \qquad f'(s_2) = -20 \neq 0 \pmod{101}.$$

Therefore, by Hensel's lemma, there is (for each $j = 1, 2$) a *unique* root r_j of $f(x)$ modulo 101^2 which is congruent to s_j modulo 101. The root r_1 is given by

$$r_1 \equiv s_1 - \frac{f(s_1)}{f'(s_1)} \equiv 10 - \frac{101}{20} \equiv 10 + 5 \cdot 101 \equiv 515 \pmod{101^2},$$

where the fact that -5 is the inverse of 20 modulo 101 has been used to derive the penultimate equation. Likewise, the root r_2 is given by

$$r_2 \equiv s_2 - \frac{f(s_2)}{f'(s_2)} \equiv -10 + \frac{101}{20} \equiv -10 - 5 \cdot 101 \equiv -515 \pmod{101^2}.$$

(Or you could just observe that the second root is necessarily the negative of the first, since you are extracting a square root.)