Math 115 Professor K. A. Ribet

First Midterm Exam September 29, 2000

This is a closed-book exam: no notes, books or calculators are allowed. Explain your answers in complete English sentences. No credit will be given for a "correct answer" that is not explained fully. In general, there is no need to simplify numerical answers.

1 *(5 points). Let a and b be positive integers for which a^4 divides b^3. Prove that a divides b.*

This is like problem 10 in §3.4, which was assigned for homework. Briefly, we have to show, for each prime p, that the exponent of p in the prime factorization of a is at most the exponent of p in the prime factorization of b. Let e and f be the two exponents in question. The given divisiblity implies that $4e \leq 3f$, so that $e \leq 3f/4$. Since f is non-negative, we get $e \leq f$, as desired.

2 *(10 points). Let $f(x) = x^2 - x - 1$. Here are some values of f:*

i	0	1	2	3	4	5	6	7	8	9	10	$\cdots$
$f(i)$	-1	-1	1	5	11	19	29	41	55	71	89	$\cdots$.

Find integers a and b so that $f(a)$ and $f(b)$ are both divisible by 11^2 but so that $a - b$ is not divisible by 11^2. Find the number of solutions mod $5 \cdot 11^2$ to the congruence $f(x) \equiv 0$ mod $5 \cdot 11^2$.

The solutions mod 11 to the congruence $f(x) \equiv 0$ mod 11 can be read off the table: they are 4 mod 11 and 8 mod 11. If r is either 4 or 8, then $f'(r) = 2r - 1$ is non-zero mod 11. Thus Hensel's lemma applies to show that r lifts uniquely to a root of f mod 11^k for $k = 2, 3, \ldots$. We have to find the lifts: Computing, I found that 37 is a lift of 4 mod 11 at which f vanishes mod 121 and that $-36 \equiv 85$ mod 121 is a lift of 8 mod 11 on which f vanishes mod 121. Thus we can take $a = 37$ and $b = 85$.

The number of roots mod $5 \cdot 121$ is the product of the number of roots mod 5 and the number of roots mod 121 (because of the Chinese remainder theorem). The table shows that there is only one root mod 5, namely 3. (It occurs twice in the table, at 3 and at 8.) Hence the number of solutions mod $5 \cdot 121$ is $1 \cdot 2 = 2$.

3 *(3 points). Let* $m = 173 \cdot 193$. *Find positive integers* a *and* b *with* $\sqrt{m} < b < \dfrac{m+1}{2}$ *for which* $m = b^2 - a^2$.

If $m = rs$, then $m = \left(\dfrac{r+s}{2}\right)^2 - \left(\dfrac{r-s}{2}\right)^2$. We take $r = 193$ and $s = 173$. This gives $b = 183$ and $a = 10$.

4 *(5 points). Use the identity*

$$1 = 89 \cdot 24 - 61 \cdot 35 \qquad (*)$$

to solve the simultaneous congruences

$$x \equiv \begin{cases} 3 & \textit{mod } 89 \\ 12 & \textit{mod } 61. \end{cases}$$

The identity (*) certainly implies that 89 and 61 are relatively prime. Hence the set of x satisfying the two congruences is a residue class mod $61 \cdot 89 = 5429$. One member of this residue class is the integer $-3 \cdot 61 \cdot 35 + 12 \cdot 89 \cdot 24 = 19227$. This number is congruent to 2940 mod 5429.

5 *(4 points). Using (*), find integers* a *and* b *with* $1 = 24a + 35b$ *and* $|a|$ *as small as possible.*

We have $1 = 24a + 35b$ when $a = 89$ and $b = -61$. The general pair (a, b) is gotten by adding $24t$ to 61 and subtracting $35t$ from 89; here t is an arbitrary integer. We thus have to find the integer $89 - 35t$ with smallest absolute value. This integer is $89 - 35 \cdot 3 = -16$.

6 *(3 points). Using (*) yet again, solve the congruence* $35x \equiv 2$ *mod 89.*

You can see from (*) that $35 \cdot (-61)$ is congruent to 1 mod 89. Hence if $x \equiv -2 \cdot 61$ mod 89, then $35x \equiv 2$ mod 89. We have $-2 \cdot 61 = -122 \equiv 56$ mod 89, so 56 is perhaps the best answer here.

NB: If you find mistakes in this write-up, please let me know by e-mail and I'll make the necessary changes.