Number Theory
McGill 189-346/377 B
Solutions to Final Exam

1. No. Note that 4713 has prime factorization $3 \cdot 1571$, and so 1066 is a square modulo 4713 if and only if it is a square modulo both 3 and 1571. To begin with, $1066 \equiv 1 \pmod 3$, so 1066 is a square modulo 3. Next, factor $1066 = 2 \cdot 13 \cdot 41$, and so
$$\left(\frac{1066}{1571}\right) = \left(\frac{2}{1571}\right)\left(\frac{13}{1571}\right)\left(\frac{41}{1571}\right).$$
Since $1571 \equiv 3 \pmod 8$, we have $\left(\frac{2}{1571}\right) = -1$. By repeated application of quadratic reciprocity,
$$\left(\frac{13}{1571}\right) = \left(\frac{1571}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1,$$
while
$$\left(\frac{41}{1571}\right) = \left(\frac{1571}{41}\right) = \left(\frac{1571}{41}\right) = \left(\frac{13}{41}\right) = \left(\frac{41}{13}\right) = \left(\frac{2}{13}\right) = -1.$$
Hence
$$\left(\frac{1066}{1571}\right) = (-1)\cdot(-1)\cdot(-1) = -1,$$
and 1066 is a square modulo neither 1571 nor 4713.

2. As we saw in class, one intelligent way to study a real number is to study its continued fraction expansion. This is especially true of a real number known to be quadratic, since quadratic numbers have periodic continued fraction expansions. In this case, if we compute the continued fraction of the truncation 3.806659275674, we find the expansion
$$[3, 1, 4, 5, 1, 4, 5, 1, 4, 5, 1, 4, 5, 2, \ldots],$$
and we might reasonably guess that the number I'm thinking of is $\beta = [3, \overline{1, 4, 5}]$. (Note that even with a calculator where you can enter only eight digits after the decimal point, one can still compute accurately as far as $[3, 1, 4, 5, 1, 4, 5, 1, 4, \ldots]$.)

   We know that the number $\alpha = [\overline{1, 4, 5}]$ satisfies $\alpha = [1, 4, 5, \alpha]$. The convergents to this continued fraction are, in order, $s_0 = 1/1$, $s_1 = 5/4$, $s_2 = 26/21$, $s_3 = \alpha = (26\alpha + 5)/(21\alpha + 4)$. Thus $21\alpha^2 - 22\alpha - 5 = 0$, and solving the quadratic equation yields $\alpha = (11 + \sqrt{226})/21$. Then $\beta = 3 + 1/\alpha = 3 + (\sqrt{226} - 11)/5 = (4 + \sqrt{226})/5$. And if you guessed that I'm thinking of
$$(4 + \sqrt{226})/5 = 3.8066592756745816541757861 12\ldots$$
then you'd be right!

3. Here's one way to do it. First, we reinterpret the condition that 7 is a square (mod p) as a congruence. In fact, we saw in class that for distinct odd primes p and q, quadratic reciprocity tells us: q is a square (mod p) if and only if $p \equiv \pm(\text{an odd square}) \pmod{4q}$. In this particular case, we learn that 7 is a square (mod p) if and only if $p \equiv \pm1, \pm9, \pm25 \pmod{28}$.

   Hence the first two conditions of the problem amount to: $p \equiv \pm1, \pm9, \pm25 \pmod{28}$ and $p \equiv 8 \pmod{15}$. Now 15 and 28 are relatively prime, and $15 \cdot 28 = 420$, so by the Chinese Remainder Theorem our conditions are equivalent to a condition (mod 420). Observe that $28 \cdot 7 = 196 \equiv 1 \pmod{15}$ while $225 = 15 \cdot 15 \equiv 1 \pmod{28}$. It follows that
$$\begin{aligned}
p \equiv 1 \pmod{28}, p \equiv 8 \pmod{15} &\Leftrightarrow p \equiv 1 \cdot 225 + 8 \cdot 196 \equiv 113 \pmod{420}\\
p \equiv -1 \pmod{28}, p \equiv 8 \pmod{15} &\Leftrightarrow p \equiv -1 \cdot 225 + 8 \cdot 196 \equiv 83 \pmod{420}\\
p \equiv 9 \pmod{28}, p \equiv 8 \pmod{15} &\Leftrightarrow p \equiv 9 \cdot 225 + 8 \cdot 196 \equiv 233 \pmod{420}\\
p \equiv -9 \pmod{28}, p \equiv 8 \pmod{15} &\Leftrightarrow p \equiv -9 \cdot 225 + 8 \cdot 196 \equiv 383 \pmod{420}\\
p \equiv 25 \pmod{28}, p \equiv 8 \pmod{15} &\Leftrightarrow p \equiv 25 \cdot 225 + 8 \cdot 196 \equiv 53 \pmod{420}\\
p \equiv -25 \pmod{28}, p \equiv 8 \pmod{15} &\Leftrightarrow p \equiv -25 \cdot 225 + 8 \cdot 196 \equiv 143 \pmod{420}.
\end{aligned}$$

Edvidently 42 is a divisor of 420, so the class of $p \pmod{420}$ determines the remainder when p is divided by 42. The remainders when 113, 83, 233, 383, 53, and 143 are divided by 42 are, respectively, 29, 41, 23, 5, 11, 17. The only single-digit remainder corresponds to $p \equiv 383 \pmod{420}$, which is therefore the answer to this question.

4. (a) Set $s_{a,b} = F_b F_{a-1} - F_a F_{b-1}$, defined for $a, b \geq 0$. Now for $a > 0$, we compute

$$\begin{aligned} s_{a,b} + s_{a-1,b} &= (F_b F_{a-1} - F_a F_{b-1}) + (F_b F_{a-2} - F_{a-1} F_{b-1}) \\ &= F_b(F_{a-1} + F_{a-2}) - (F_a + F_{a-1}) F_{b-1} \\ &= F_b F_a - F_{a+1} F_{b-1} \\ &= s_{a+1,b} \end{aligned}$$

Moreover, $s_{0,b} = F_b F_{-1} - F_0 F_{b-1} = F_b \cdot 1 - 0 \cdot F_{b-1} = F_b$, while $s_{1,b} = F_b F_0 - F_1 F_{b-1} = F_b \cdot 0 - 1 \cdot F_{b-1} = -F_{b-1}$. Hence

$$s_{2,b} = s_{1,b} + s_{0,b} = -F_{b-1} + F_b = F_{b-2}\,,$$

$$s_{3,b} = s_{2,b} + s_{1,b} = F_{b-2} + (-F_{b-1}) = -F_{b-3}\,,$$

and continuing in this fashion, an easy induction shows that $s_{a,b} = (-1)^a F_{b-a}$. (Note that we need two base cases to get this induction to work!)

(b) It follows immediately from the relation in (a) that if $n \mid F_b$ and $n \mid F_a$, then $n \mid F_{b-a}$. Another application of the relation (now using $b-a$, a instead of b, a) shows that $n \mid F_{b-2a}$, and interating this step we see that $n \mid F_{b-a}, F_{b-2a}, \ldots, F_{b-qa} = F_r$.

(c) **Solution 1:** Again we use an induction: suppose that F_a is known to divide F_{ka} (which is certainly true for $k = 1$). We will show that F_a divides $F_{(k+1)a}$. Indeed, we can apply part (a) with $b = (k+1)a$ and rewrite to find: $F_{(k+1)a} F_{a-1} = F_a F_{b-1} + (-1)^a F_{ka}$. By our inductive assumption, F_a divides the right-hand side, and so it divides the left-hand side as well. The crucial point now is that F_a and F_{a-1} are relatively prime, so the fact that F_a divides $F_{(k+1)a} F_{a-1}$ does indeed imply that F_a divides $F_{(k+1)a}$.

Solution 2: Consider the Fibonacci sequence $\pmod{F_a}$. The sequence begins $0, 1, \ldots,$ and reaches 0 again at the a^{th} term. At the a^{th} term, the sequence $\pmod{F_a}$ continues $0, F_{a+1}, \ldots,$ and so the values of the Fibonacci sequence $\pmod{F_a}$ from terms a to $2a$ will simply be F_{a+1} times the values of the Fibonacci sequence $\pmod{F_a}$ from terms 0 to a. It follows instantly that $F_{2a} \equiv 0 \pmod{F_a}$, and repeated application of this argument shows that $F_{ka} \equiv 0 \pmod{F_a}$ for all positive integers k.

(d) By part (c), $F_{(a,b)}$ divides both F_a and F_b, so it must divide (F_a, F_b). Now suppose that the Euclidean algorithm applied to b and a looks like

$$\begin{aligned} b &= q_0 a + r_0 \\ a &= q_1 r_0 + r_1 \\ &\vdots \\ r_k &= q_{k+2} r_{k+1} + 0 \end{aligned}$$

so that $(a, b) = r_{k+1}$. If n divides F_a and F_b, then part (b) tells us that n divides F_{r_0}. Since now n divides F_a and F_{r_0}, we find by (b) that n divides F_{r_1}. Continuing, we obtain $n \mid F_{r_{k+1}} = F_{(a,b)}$. This shows $(F_a, F_b) \mid F_{(a,b)}$, and since we have already shown the reverse, the desired conclusion follows.

5. (a) Factor $936 = 2^3 \cdot 3^2 \cdot 13$, so by the Chinese Remainder Theorem we have

$$\mathbb{Z}/936\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus Z/13\mathbb{Z}\,.$$

We saw that this implies

$$(\mathbb{Z}/936\mathbb{Z})^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/9\mathbb{Z})^\times \times (\mathbb{Z}/13\mathbb{Z})^\times\,.$$

Our study of primitive roots showed that $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$ (not C_4), that $(\mathbb{Z}/9\mathbb{Z})^\times \cong C_6$ (not C_8! remember, $\phi(9) = 6$), and that $(\mathbb{Z}/13\mathbb{Z})^\times \cong C_{12}$. Hence $(\mathbb{Z}/936\mathbb{Z})^\times \cong C_2 \times C_2 \times C_6 \times C_{12}$.

Note that this is not the only acceptable answer: for example, $C_6 \cong C_2 \times C_3$, and so $(\mathbb{Z}/936\mathbb{Z})^\times \cong C_2 \times C_2 \times C_2 \times C_3 \times C_{12}$ as well. This manoeuver gives several other equivalent lists of d_i: $2,2,2,3,3,4$, or $2,2,3,4,6$, or $2,4,6,6$, or $2,2,2,3,12$, or $2,2,6,12$.

(b) The number of elements of order *dividing* 4 in $C_2 \cdots C_2 \cdot C_6 \cdot C_{12}$ is given by $2 \cdot 2 \cdot 2 \cdot 4 = 32$. The number of elements of order exactly 2 is given by $2 \cdot 2 \cdot 2 \cdot 2 = 16$. Hence the number of elements of order exactly 4 is $32 - 16 = 16$.

6. (a) One may compute $\sqrt{61} = [7,1,4,3,1,2,2,1,3,4,1,14,\ldots]$, and since we knew that 14 would be the element in this continued fraction immediately before the continued fraction begins to repeat, it is reasonable to guess that $\sqrt{61} = [7,\overline{1,4,3,1,2,2,1,3,4,1,14}]$. We can actually confirm this by checking that the convergent $[7,1,4,3,1,2,2,1,3,4,1]$ yields a solution to Pell's equation $x^2 - 61y^2 = \pm 1$, because we know that *only* the convergents which are cut off at the very end of the repeating portion will yield solutions.

So as usual we compute $p_{-1}/q_{-1} = 1/0$, $p_0/q_0 = 7/1$, $p_1/q_1 = 8/1$, $p_2/q_2 = 39/5$, and so on, until $p_{10}/q_{10} = 29718/3805$. And indeed we find $29718^2 - 61 \cdot 3805^2 = -1$, confirming our suspicion about the continued fraction of $\sqrt{61}$ and yielding the smallest solution of Pell's equation for $N = 61$.

However, the question at hand asks for the smallest solution of $x^2 - 61y^2 = +1$, and so we aren't quite done yet. One way to finish this is to continue computing out to p_{21}/q_{21}; instead we use the trick mentioned in class, namely that if $z = 29718 + 3805\sqrt{61}$, then the "coefficients" in z^2 will be the solution we're looking for. Computing, we find $z^2 = 1766319049 + 226153980\sqrt{61}$, and indeed $1766319049^2 - 61 \cdot 226153980^2 = 1$. This is our solution.

(b) To show that $x^2 - 34y^2 = -1$ has no solutions, it suffices to show that the smallest solution to $x^2 - 34y^2 = \pm 1$ has a $+1$, not a -1; or, equivalently, that the period length of the continued fraction of $\sqrt{34}$ is even.

So we compute the continued fraction expansion of $\sqrt{34}$, which begins

$$[5,1,4,1,10,1,4,1,10,\ldots].$$

The period length appears to be 4, but we cannot quite claim to be done, because to be rigorous we need to prove that this is really the continued fraction expansion of $\sqrt{34}$. As before, we can do this by checking that $[5,1,4,1]$ yields a solution to Pell's equation for $N = 34$. Indeed $p_3/q_3 = 35/6$ and $35^2 - 34 \cdot 6^2 = +1$, and we're done. (Note, by the way, that we haven't been able to avoid checking directly that the smallest solution to Pell's equation for $N = 34$ has a $+1$.)

(c) For example, $(5/3)^2 - 34(1/3)^2 = -1$.

7. (a) We look for solutions of $b^2 - 4ac = -160$ yielding reduced binary quadratic forms. Note that b must be even, and $|b| \le a \le \sqrt{160/3} < 8$, so we need to consider $|b| = 0,2,4,6$. In any case, $ac = 40 + b^2/4$.

$b = 0$: we have $ac = 40$. We need $(a,c) = 1$ and $a \le c$, so the solutions are $(a,c) = (1,40), (5,8)$, and we obtain the forms $x^2 + 40y^2$, $5x^2 + 8y^2$.

$|b| = 2$: we have $ac = 41$, forcing $(a,c) = (1,41)$. But then $a < |b|$, so the resulting forms are not reduced.

$|b| = 4$: we have $ac = 44$. Since $a \le c$ the possibilities are $(a,c) = (1,44), (2,22), (4,11)$. We eliminate $(a,c) = (1,44)$ because we need $|b| < a$, and $(a,c) = (2,22)$ because the resulting form would not be primitive. Finally, when $(a,c) = (4,11)$ we must take $b = 4$ and not $b = -4$ (because $|b| = a$), giving the form $4x^2 + 4xy + 11y^2$.

$|b| = 6$: we have $ac = 49$. The possibilities are $(a, c) = (1, 49), (7, 7)$, and the condition $|b| < a$ eliminates $(1, 49)$. When $(a, c) = (7, 7)$ we must take $b = 6$ and not $b = -6$, because $a = c$. We obtain the form $7x^2 + 6xy + 7y^2$.

Hence there are four reduced forms of discriminant $D = -160$: $x^2 + 40y^2$, $5x^2 + 8y^2$, $4x^2 + 4xy + 11y^2$, and $7x^2 + 6xy + 7y^2$.

(b) Observe that all of the above forms either have $b = 0$, $b = a$, or $a = c$. The main theorem of genus theory then tells us that every form of discriminant -160 is *unique in its genus.* Hence, by a theorem in Cox's book, if f is a form of discriminant -160 and p is a prime not dividing -160, then $f(x, y)$ represents p if and only if $f(x, y) \equiv p \pmod{160}$ has a solution. Moreover, for each such f, the set of congruence classes represented by f is a coset of the set of congruence classes represented by the principal form $x^2 + 40y^2$.

Note that $40y^2 \equiv 0, 40 \pmod{160}$, and so the set of congruence classes represented by the principal form is precisely the set of congruence classes $b^2, b^2 + 40 \pmod{160}$ for $(b, 160) = 1$. Now $5x^2 + 8y^2$ represents 13 (we can't use 5 or 8 because these divide 160) and so the coset represented by $5x^2 + 8y^2$ is the coset of classes $13b^2, 13(b^2 + 40) \pmod{160}$. Noting that $13 \cdot 40 \equiv 40 \pmod{160}$, we are done.

8. (a) Choose any $\delta > 0$. Suppose that $|\alpha - p/q| \leq \delta$. Since the derivative $f'(x)$ is continuous, we can choose M such that $|f'(y)| < M$ for $y \in [\alpha - \delta, \alpha + \delta]$. By the mean value theorem, there exists ξ between α and p/q such that

$$\begin{aligned} |f(\alpha) - f(p/q)| &= |\alpha - p/q||f'(\xi)| \\ &< |\alpha - p/q|M \end{aligned}$$

because $\xi \in [\alpha - \delta, \alpha + \delta]$.

However, $f(x)$ is a polynomial of degree n with integer coefficients and with no rational roots, and it follows from these facts that $f(p/q) = (\text{non-zero integer})/q^n$. Since $f(\alpha) = 0$, putting all this together we obtain:

$$1/q^n \leq |f(\alpha) - f(p/q)| < M|\alpha - p/q|$$

or, rearranging,

$$|\alpha - p/q| > \frac{1/M}{q^n}.$$

Recall that this holds only when $|\alpha - p/q| \leq \delta$. But when $|\alpha - p/q| > \delta$, then since $q \geq 1$ it is certainly true that

$$|\alpha - p/q| > \frac{\delta}{q^n}.$$

Hence taking $c = \min(1/M, \delta)$ we obtain an inequality valid for all p/q.

(b) This is clearly the contrapositive of part (a).

(c) We make use of a slightly strengthened version of (b). To wit, we note that if there exists a sequence $c_n \to 0$ and integers p_n, q_n such that $|\alpha - p_n/q_n| < c_n/q_n^n$ for all n then α is transcendental. Indeed, choose any $c > 0$. Since $c_n \to 0$, we may always choose m sufficiently large that $c_m < c \leq c q_m^{m-n}$, in which case $c_m/q_m^m < c/q_m^n$. For this m, we have

$$\left|\alpha - \frac{p_m}{q_m}\right| < \frac{c_m}{q_m^m} < \frac{c}{q_m^n}.$$

Hence the criterion in (b) is satisfied as well.

Now for $\eta = \sum \frac{1}{10^{k!}}$, set $q_n = 10^{n!}$ and $p_n = \sum_{k=0}^{n} 10^{n!-k!}$. Then

$$|\eta - p_n/q_n| < \frac{2}{10^{(n+1)!}} = \frac{2/10^{n!}}{q_n^n}$$

and so taking $c_n = 2/10^{n!}$ we are done.

9. The argument here is surprisingly short. We simply list all of the reduced binary quadratic forms of discriminant $D = 1 - 4n$. The coefficients of a reduced binary quadratic form satisfy $b^2 - 4ac = 1 - 4n$, so b must be odd. Writing $|b| = 2b' + 1$, we find $(2b' + 1)^2 - 4ac = 1 - 4n$, and expanding and rearranging yields $ac = (b')^2 + (b') + n$. Moreover, since we are looking for reduced forms, we need only search for $a \leq \sqrt{(4n-1)/3} < 2\sqrt{n/3}$; and because $2b' + 1 = |b| \leq a$, we are testing only b' lying in the given range $0 \leq b' < \sqrt{n/3}$. We are given that for each such b', the number $(b')^2 + (b') + n = ac$ is prime, and so each time the only possibility for (a, c) has $a = 1$. But $a = 1$ implies $|b| = 1$ since $|b| \leq a$; then $a = |b|$ forces $b > 0$, so $b = 1$. Then $c = n$, and so the only reduced binary quadratic form of discriminant $1 - 4n$ is $x^2 + xy + ny^2$. Hence the class number $h(1 - 4n) = 1$, and we saw (in lecture, and in Cox) that in this situation, the polynomial $x^2 + x + n$ is prime for $0 \leq x < n - 1$.

10. (b) Let's discuss part (b) first, since it will illuminate the rest of the problem. We want to determine when 2^d is congruent modulo 1000 to some number N among 111, 112, 121, 122, 211, 212, 221, 222. The first observation is that N is going to have to be 112. Indeed, $2^d \equiv N \pmod{1000}$ implies $2^d \equiv N \pmod 8$. Evidently $d > 3$, so $2^d \equiv 0 \pmod 8$, and hence $N \equiv 0 \pmod 8$. Yet 112 is the only one of the above numbers divisible by 8, and so N is going to have to be 112.

    Now we want to solve $2^d \equiv 112 \pmod{1000}$. By the Chinese remainder theorem, this amounts to $2^d \equiv 112 \pmod{125}$ and $2^d \equiv 112 \pmod 8$. The latter, we have already seen, is true provided $d \geq 3$. For the former, we can see quickly that there *exists* a solution. Indeed, 2 is a primitive root modulo 25: since $\phi(25) = 20$, we see this by checking that $2^{20/2} = 1024 \not\equiv 1 \pmod{25}$, and that $2^{20/5} = 16 \not\equiv 1 \pmod{25}$. We saw in class that if a is a primitive root modulo p^2 (for an odd prime p), then a is a primitive root modulo p^n for all n. Hence 2 is a primitive root modulo 5^n for all n, and in particular 2 is a primitive root modluo 125. Since $(112, 125) = 1$, certainly $2^d \equiv 112 \pmod{125}$ has a solution. We now need to find the smallest solution (with $d \geq 3$).

    We do this efficiently by stepping from 25 to 125. What we mean by this is, we first observe that $2^d \equiv 112 \equiv 12 \pmod{25}$ if and only if $d \equiv 9 \pmod{20}$. This is because $d = 9$ solves $2^d \equiv 12 \pmod{25}$, and any two solutions must differ by a multiple of $\phi(25) = 20$. Therefore the smallest solution of $2^d \equiv 112 \pmod{125}$ will be found in the sequence $9, 29, 49, \ldots$. We can calculate

$$2^{20} = (1024)^2 \equiv 24^2 \equiv 76 \pmod{125}$$

    and so, successively,

$$\begin{aligned} 2^9 &\equiv 12 \pmod{125} \\ 2^{29} &\equiv 12 \cdot 76 \equiv 37 \pmod{125} \\ 2^{49} &\equiv 37 \cdot 76 \equiv 62 \pmod{125} \\ 2^{69} &\equiv 62 \cdot 76 \equiv 87 \pmod{125} \\ 2^{89} &\equiv 87 \cdot 76 \equiv 112 \pmod{125} \end{aligned}$$

    and so $d = 89$ is our smallest solution.

    (a) Now we wish to see that there exists a solution for arbitrary $n > 3$. As in (b), we need to see that there is an string N consisting of n digits, all 1 or 2, so that $2^d \equiv N \pmod{10^n}$ has a solution. Since N has n digits, it follows that $2^d > 10^{n-1}$, and certainly this entails $d \geq n$.

    Again by the Chinese Remainder Theorem, the equation $2^d \equiv N \pmod{10^n}$ has solutions if and only if $2^d \equiv N \pmod{5^n}$ and $2^d \equiv N \pmod{2^n}$ can be solved simultaneously. We have already seen that 2 is a primitive root modulo 5^n, and since certainly $(N, 5) = 1$, the former equation always has (infinitely many) solutions. Moreover, since $d \geq n$ the second equation amounts simply to $N \equiv 0 \pmod{2^n}$. Therefore, if N can be found such that

$N \equiv 0 \pmod{2^n}$, the this latter equation is automatically satisfied, and we can choose our d to be any solution $d \geq n$ to the former equation.

So, we have reduced the problem to proving simply that N may be chosen so that it is divisible by 2^n. This can be done directly by induction without too much difficulty, but to do this quickly, we resort to outright trickery. Noting that there are 2^n different possible strings of 1s and 2s, i.e., 2^n different possible values for N, we must only show that all these possibilities are distinct modulo 2^n. But this is clear: suppose that the right-most digit where N and N' differ is the 10^k-place. Then $N - N'$ has 0 in the $10^0, \ldots, 10^{k-1}$ places, and an odd digit in the 10^k-place (since one of N, N' has a 1 in that place and the other has a 2). Hence 2^k divides $N - N'$ but 2^{k+1} does not, and since $k < n$, we see that $N \not\equiv N' \pmod{2^n}$.