Math 445
Handy facts for the second exam

Don't forget the handy facts from the first exam!

Quadratic Reciprocity.

Quadratic Residues: If $x^2 \equiv a \pmod{n}$ has a solution, a is a *quadratic residue* modulo n . If it doesn't, a is a *quadratic non-residue* modulo n . Euler's Criterion gives us a test: if p is a prime, then a is a quadratic residue mod $n \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

The *Legendre symbol*; for p an odd prime,
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}$$

By Euler's criterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Basic facts: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, and $\left(\frac{a+pk}{p}\right) = \left(\frac{a}{p}\right)$.

Lemma of Gauss: Let p be an odd prime and $(a,p)=1$. For $1 \leq k \leq \frac{p-1}{2}$ let $ak = pt_k + a_k$ with $0 \leq a_k \leq p-1$. Let $A = \{k : a_k > \frac{p}{2}\}$, and let $n = |A| =$ the number of elements in A . Then $\left(\frac{a}{p}\right) = (-1)^n$.

Theorem: Let p be an odd prime and $(a,2p)=1$ (i.e., $(a,p)=1$ and a is odd). Let $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{aj}{p} \rfloor$. Then $\left(\frac{a}{p}\right) = (-1)^t$.

Along the way, this gives: $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$. And putting it all together, we get

Gauss' Law of Quadratic Reciprocity:

If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$.

The facts

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$ for distinct odd primes, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
allow us to carry out the calculations of Legendre symbols much more simply than Euler's criterion would.

For Q odd and $(A,Q)=1$, if $Q = q_1 \cdots q_k$ is the prime factorization of Q, then the *Jacobi symbol* $\left(\frac{A}{Q}\right)$ is defined to be $\left(\frac{A}{Q}\right) = \left(\frac{A}{q_1}\right) \cdots \left(\frac{A}{q_k}\right)$.

Some basic properties:

If $(A,Q) = 1 = (B,Q)$ then $\left(\frac{AB}{Q}\right) = \left(\frac{A}{Q}\right)\left(\frac{B}{Q}\right)$

If $(A,Q) = 1 = (A,Q')$ then $\left(\frac{A}{QQ'}\right) = \left(\frac{A}{Q}\right)\left(\frac{A}{Q'}\right)$

If $(PP', QQ') = 1$ then $\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$

Warning! If Q is not prime, then $\left(\frac{A}{Q}\right) = 1$ does *not* mean that $x^2 \equiv A \pmod{Q}$ has a solution. Most of it's properties are identical to the Legendre symbol:

If Q is odd, then $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$

If Q is odd, then $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$

If P and Q are both odd, and $(P, Q) = 1$, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(\frac{P-1}{2})(\frac{Q-1}{2})}$

Since the Jacobi symbol has essentially the same properties as the Legendre symbol, we can compute them in essentially the same way; extract factors of 2 from the top (and -1), and use reciprocity to compute the rest. The advantage: we don't need to factor the top any further, any odd number will work fine.

Interlude: $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

We showed: the sum of the reciprocals of the primes $\leq N$ is $\geq \ln(\ln(N)) - 4$. In fact, as $n \to \infty$, $\displaystyle (\sum_{p \text{ prime}, p \leq n} \frac{1}{p}) - \ln(\ln(n))$ converges to a finite constant M, known as the *Meissel-Mertens constant*. It's value is, approximately, 0.26149721284764278... .

Continued Fractions.

If we look at each line of the calculation of g.c.d of a and b,

$$a = bq_0 + r_0,\ b = r_0q_1 + r_1,\ \dots,\ r_{n-2} = r_{n-1}q_n + r_n,\ r_n = r_{n-1}q_{n+1} + 0$$

they can we re-written as

$$\frac{a}{b} = q_0 + \frac{r_0}{b}, \frac{b}{r_0} = q_1 + \frac{r_1}{r_0}, \dots \frac{r_{n-2}}{r_{n-1}} = q_n + \frac{r_n}{r_{n-1}}, \frac{r_n}{r_{n-1}} = q_{n+1}$$

When we put these together, we get a *continued fraction expansion* of a/b

$$(*) \qquad \frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_{n+1}}}}}$$

which, for the sake of saving space, we will denote $\langle q_0, q_1, \dots, q_{n+1}\rangle$. Note that, conversely, given a collection $q_0, \dots, q_{n+1}$ of integers, we can construct a rational number, which we denote $\langle q_0, q_1, \dots, q_{n+1}\rangle$, by the formula (*).

Formally, we can try to do the same thing with any real number x; i.e, "compute" the g.c.d. of x and 1 :

$x = 1 \cdot a_0 + r_0$, $1 = r_0a_1 + r_1$, $\dots$, $r_{n-2} = r_{n-1}a_n + r_n$, where the a_i's are integers.

Unlike for the rational number a/b, if x is irrational, we shall see that this process does not terminate, giving us an "infinite" continued fraction expansion of x, $\langle a_0, a_1, a_2 \dots\rangle$. Our main goal is to figure out what this sequence of integers means!

First, a slightly different perspective:

$x = a_0 + r_0$ with $0 \leq r_0 < 1$ means $a_0 = \lfloor x \rfloor$ is the largest integer $\leq x$; $\lfloor \text{blah} \rfloor$ is the *greatest integer function*. $1 = r_0a_1 + r_1$ with $0 \leq r_1 < r_0$ means $1/r_0 = a_1 + (r_1/r_0) = a_1 + x_1$ with $0 \leq x_1 < 1$, so $q_1 = \lfloor 1/r_0 \rfloor$. In general, the process of extracting the continued fraction expansion of x looks like:

(**) $\quad x = \lfloor x \rfloor + r_0 = a_0 + r_0, \quad 1/r_0 = \lfloor 1/r_0 \rfloor + r_1 = a_1 + r_1, \ldots,$
$\quad 1/r_{n-1} = \lfloor 1/r_{n-1} \rfloor + r_n = a_n + r_n, \ldots$

If we stop this at any finite stage, then we can, just as in the case of a rational number a/b, reassemble the pieces to give

$$x = \langle a_0, a_1, \ldots, a_{n-1}, a_n + r_n \rangle = \langle a_0, a_1, \ldots, a_{n-1}, a_n, 1/r_n \rangle$$

If we ignore the last r_n, we find that $\langle a_0, a_1, \ldots, a_{n-1}, a_n \rangle$ is a rational number (proof: induction on n), called the n^{th} *convergent* of x. The integers a_n are called the n^{th} *partial quotients* of x. Note that since $0 \leq r_0 < 1$, $1/r_0 > 1$, so $a_1 \geq 1$. This is true for all later calculations, so $a_i \geq 1$ for all $i \geq 1$. This sort of continued fraction expansion is what is called *simple*. We will, in our studies, only deal with simple continued fractions.

For example, we can compute that, for $x = \sqrt{2}$, $a_0 = 1$, $x_0 = \sqrt{2} - 1$, $1/r_0 = \sqrt{2} + 1$, $a_1 = 2$, $r_1 = \sqrt{2} - 1 = r_0$, so the pattern will repeat, and $\sqrt{2}$ has continued fraction expansion $\langle 1, 2, 2, \ldots \rangle$. By computing some partial quotients, one can show that π has expansion that begins $\langle 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, \ldots \rangle$. Euler showed that $e = \langle 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \ldots \rangle$.

By looking at the expression for a continued fraction, that we started with, it should be apparent that

$$\langle a_0, a_1, \ldots, a_{n-1}, a_n \rangle = \langle a_0, a_1, \ldots, a_{n-1} + \frac{1}{a_n} \rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_{n-1}, a_n \rangle}$$

From this it follows, for example, that $\langle a_0, a_1, \ldots, a_{n-1}, a_n \rangle = \langle a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1 \rangle$. But these are the only such equalities:

Prop: If $\langle a_0, a_1, \ldots, a_n \rangle = \langle b_0, b_1, \ldots, b_m \rangle$ and $a_n, b_m > 1$, then $n = m$ and $a_i = b_i$ for all $i = 0, \ldots, n$.

Computing $\langle a_0, a_1, \ldots, a_n \rangle$ from $\langle a_0, a_1, \ldots, a_{n-1} \rangle$:

$\langle a_0, a_1, \ldots, a_n \rangle = \dfrac{h_n}{k_n}$, where $h_{-2} = 0, k_{-2} = 0, h_{-1} = 1, k_{-1} = 0$, and for $i \geq 0$,

$$h_i = a_i h_{i-1} + h_{i-2} \text{ and } k_i = a_i k_{i-1} + k_{i-2}.$$

The proof is by induction. This, in turn implies:

For every $i \geq 0$, $h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}$ (which implies that $(h_i, k_i) = 1$), and $h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i$.

Note: None of these formulas actually require that the a_i's be integers.

for $x = \langle a_0, a_1, \ldots, a_{n-1}, a_n + r_n \rangle = \langle a_0, a_1, \ldots, a_{n-1}, a_n, \dfrac{1}{r_n} \rangle$, if we set

$$\langle a_0, a_1, \ldots, a_{n-1}, a_n \rangle = x_n,$$

then these formulas imply that

$$x_{2n} < x_{2n+2} \text{ and } x_{2n-1} > x_{2n+1} \text{ for every } n, \text{ and } x_{2n} - x_{2n-1} = \frac{1}{k_{2n-1} k_{2n}}$$

And since the numerator of

$x - \langle a_0, a_1, \ldots, a_{n-1}, a_n \rangle = \langle a_0, a_1, \ldots, a_{n-1}, a_n + r_n \rangle - \langle a_0, a_1, \ldots, a_{n-1}, a_n \rangle$,

we can compute, is $r_n(h_{n-1} k_{n-2} - h_{n-2} k_{n_1})$ (and the denomenator is positive), we have that $x_{2n} < x < x_{2n+1}$. So since $x_{2n} - x_{2n-1} \to 0$ as $n \to \infty$, we find that $x_n \to x$, In particular, $|x - x_{n-1}| < |x_{n-1} - x_n| = 1/(k_{n-1} k_n)$ for every n. This implies that if the

r_n are never 0 (i.e., the continued fraction process is really an infinite one), then since $0 < |k_n(x - x_n)| = |k_n x - h_n| < 1/k_{n-1}$, we find that x is not rational.
This last observation requires us to know that the k_n are getting arbitrarily large. But note that since $a_i \geq 1$ for every $i > 0$, $k_{-1} = 0, k_0 = 1$, and $k_i = a_i k_{i-1} + k_{i-2} \geq k_{i-1} + k_{i-2}$ for every $i \geq 1$, we can see by induction that $k_n \geq$ the n^{th} Fibonacci number (which is defined by $F_i = F_{i-1} + F_{i-2}$), and the Fibonacci numbers grow very fast!
Based on these facts, we denote $x = \lim_{n\to\infty} \langle a_0, \ldots, a_n\rangle = \langle a_0, a_1, \ldots\rangle$. Then

$$\langle a_0, a_1, \ldots\rangle = a_0 + \frac{1}{\langle a_1, a_2, \ldots\rangle}$$

which in turn implies that:
If $\langle a_0, a_1, \ldots\rangle = \langle b_0, b_1, \ldots\rangle$, then $a_i = b_i$ for all i.
If $1 \leq b < k_n$, then $|x - \frac{a}{b}| \geq |x - \frac{h_n}{k_n}|$ for all integers a; in fact if $1 \leq b < k_{n+1}$, then $|bx - a| \geq |k_n x - h_n|$ for all integers a.
If $x \notin \mathbb{Q}$ and $a, b \in \mathbb{Z}$, with $|x - \frac{a}{b}| < \frac{1}{2b^2}$, then $\frac{a}{b} = \frac{h_n}{k_n}$ for some n.
Repeating continued fraction expansions: A continued fraction $\langle a_0, a_1, \ldots\rangle$ will repeat (i.e, $a_n = a_{n+m}$ for all $n \geq N$) precisely when $x_{n-1} = x_{n+m-1}$, since from (**) above, all of the calculations of the partial quotients, starting from some fixed number, will depend only on that fixed number. A real number x has a repeating continued fraction expansion if and only if x is an (irrational) root of a quadratic equation, what we call a *quadratic irrational*. In particular,
For any non-square positive integer n, $\sqrt{n} + \lfloor\sqrt{n}\rfloor = \langle\overline{2a_0, a_1, \ldots a_m}\rangle$ is *purely periodic*. This implies that $\sqrt{n} = \langle a_0, \overline{a_1, \ldots a_m, 2a_0}\rangle$

Pell's Equation.

It turns out that the continued fraction expansion of $\sqrt{n}$ can help us find the integer solutions x, y of the equation

$$(***) \qquad x^2 - ny^2 = N$$

for fixed values of n and N. This equation is known as *Pell's equation*.
First the less interesting cases. If $n < 0$, then any solution to $N = x^2 - ny^2 \geq x^2 + y^2$ has $|x|, |y| \leq \sqrt{N}$, which can be found by inspection. If $n = m^2$ for some m, then $N = x^2 - m^2y^2 = (x - my)(x + my)$, so $x - my, x + my$ both divide N, so, e.g., their sum, $2x$ divides N^2. We can then find all possible x, and so all solutions, by inspection. We now focus on finding solutions for $n \geq 1$ not a perfect square. $\sqrt{n}$ is therefore irrational.
Then if $1 \leq N \leq \sqrt{n}$ is not a perfect square, then $N = x^2 - ny^2$ implies that
$|\sqrt{n} - \frac{x}{y}| = \frac{N}{|x + \sqrt{n}y| \cdot |y|} < \frac{N}{2\sqrt{n}y^2} < \frac{1}{2y^2}$, so $\frac{x}{y} = \frac{h_m}{k_m}$ for some m.
(The same, it turns out, is true for $-\sqrt{n} \leq N \leq -1$.) But which m?
$\sqrt{n} = \langle a_0, \overline{a_1, \ldots a_m, 2a_0}\rangle$ means that $\sqrt{n} = \langle a_0, a_1, \ldots a_m, a_0 + \sqrt{n}\rangle$. In general, at any point where we stop computing the continued fraction of $\sqrt{n}$, we find that
$\sqrt{n} = \langle b_0, b_1, \ldots b_s, \frac{\sqrt{n}+a}{b}\rangle$, where $\frac{1}{r_s} = \frac{\sqrt{n}+a}{b}$

(so a and b take on only finitely many values, because r_s does). But then we can compute that

$\sqrt{n} = \dfrac{(\frac{\sqrt{n}+a}{b})h_s + h_{s-1}}{(\frac{\sqrt{n}+a}{b})k_s + k_{s-1}}$, which implies that $h_s^2 - nk_s^2 = b(h_s k_{s-1} - h_{s-1}k_s) = (-1)^{s-1}b$.

To compute the b's, we note that, by induction, $r_i = \dfrac{\sqrt{n}-m_i}{q_i}$and $\dfrac{1}{r_i} = \dfrac{q_i}{\sqrt{n}-m_i} = \dfrac{\sqrt{n}+m_i}{q_{i+1}}$, so we can inductive compute the quotients q_i from the equations

$q_{i+1} = \dfrac{n-m_i^2}{q_i}$, $a_{i+1} = \lfloor \dfrac{\sqrt{n}+m_i}{q_{i+1}} \rfloor$, and $m_{i+1} = a_{i+1}q_{i+1} - m_i$

and then $h_i^2 - nk_i^2 = (-1)^{i-1}q_{i+1}$.

In particular, solutions to $x^2 - ny^2 = 1$ exist, because $b = 1$ occurs as the denomenator of x_i for $i = m+1, 2m+1, 3m+1, \ldots$. These are either all odd (if m is even), or every other one is odd. For these values, $i-1$ is even, so $h_i^2 - nk_i^2 = b(h_i k_{i-1} - h_{i-1}k_i) = (-1)^{i-1}b = 1$.

There is an alternative approach to generating solutions to (***). If we know that $x^2 - ny^2 = N$ and $x_0^2 - ny_0^2 = 1$, then

$$(x^2 - ny^2)(x_0^2 - ny_0^2)^m = N = (x - \sqrt{n}y)(x_0 - \sqrt{n}y_0)^m (x + \sqrt{n}y)(x_0 + \sqrt{n}y_0)^m$$

But $(x^2 - ny^2)(x_0^2 - ny_0^2)^m = A - \sqrt{n}B$ for some A, B, and then $(x^2 + ny^2)(x_0^2 + ny_0^2)^m = A + \sqrt{n}B$ (because of the properties of *conjugates* of quadratic irrationals). Then

$(A - \sqrt{n}B)(A + \sqrt{n}B) = A^2 - nB^2 = N$.

Sums of four squares.

For every $n \in \mathbb{N}$, there are $x, y, z, w \in \mathbb{Z}$ so that $x^2 + y^2 + z^2 + w^2 = n$.

Elements of the proof:

$$(x_1^2 + y_1^2 + z_1^2 + w_1^2)(x_2^2 + y_2^2 + z_2^2 + w_2^2) =$$
$$(x_1x_2 + y_1y_2 + z_1z_2 + w_1w_2)^2 + (x_1y_2 - x_2y_1 + z_2w_1 - z_1w_2)^2 +$$
$$(x_1z_2 - x_2z_1 + y_1w_2 - w_1y_2)^2 + (x_1w_2 - x_2w_1 + y_2z_1 - y_1z_2)^2$$

so we may focus on primes p. $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$, so focus on odd primes. Then $0 \leq x, y \leq (p-1)/2$ and $x \neq y$ implies $x^2 \not\equiv y^2 \pmod{p}$, so for any a, x^2 and $a - y^2$, with $0 \leq x, y \leq (p-1)/2$ must have a value, mod p, in common (otherwise $x^2 + y^2 - a$ takes on $p+1$ different values, mod p). So $x^2 + y^2 \equiv -1 \pmod{p}$ has a solution. Then $x^2 + y^2 + 1^2 + 0^2 = Mp$ for some M; with the restrictions on x, y, we have $M < p$. Choose the smallest positive M with $Mp = x^2 + y^2 + z^2 + w^2$. M is odd, since otherwise (after renaming the variables to group them by parity)

$\dfrac{M}{2}p = (\dfrac{x-y}{2})^2 + (\dfrac{x+y}{2})^2 + (\dfrac{z-w}{2})^2 + (\dfrac{z+w}{2})^2$

If $M > 1$, then choose $-\dfrac{M}{2} \leq x_1, y_1, z_1, w_1 \leq \dfrac{M}{2}$ with $x \equiv x_1 \pmod{M}$, etc. then $x_1^2 + y_1^2 + z_1^2 + w_1^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{M}$, so $x_1^2 + y_1^2 + z_1^2 + w_1^2 = NM$ with (from the restrictions on x_1, etc.) $N < M$. Then

$NM^2p = (x_1^2+y_1^2+z_1^2+w_1^2)(x^2+y^2+z^2+w^2) =$ a sum of four squares with, we can compute, every term a multiple of M! Dividing through by M^2, we find that Np is a sum of four squares, with $N < M$, contradicting the choice of M. So $M = 1$, and we are done.

Geometric solutions to quadratic equations.

For equations such as $x^2 + 10y^2 = 19z^2$ where we know one solution (like (3,1,1)), we can find all solutions using a geometric process. Setting $X = x/z$, $Y = y/z$, our equation becomes

$$(****) \qquad X^2 + 10Y^2 = 19 \text{ (in this case, an ellipse)}$$

for which we know one (rational) solution; (3,1). Our goal is now to find all other *rational* solutions (the denomenator will be our z). But if we imagine having another rational solution (a, b), then the line through $(3, 1)$ (in our case) and (a, b) will have rational slope. If we take the equation for this line and plug it into (****), we get a quadratic equation with (because of the rational slope) rational coefficients, for which we know one, rational, solution (in our case, $X = 3$). The other solution must therefore be rational, and the corresponding point on the line then has rational coordinates. In our example, this procedure looks like

$Y = r(X-3)+1$, so $x^2+10(r(X-3)+1)^2 = 19$, i.e., $(X^2-9)+10r^2(X-3)^2+20r(X-3) = 0$, i.e., $(X-3)(X+3+10r^2X-30r^2+20r) = 0$. So $X = 3$ or $(10r^2+1)X-(30r^2-20r-3) = 0$, i.e., (setting $r = a/b$)

$$X = \frac{30r^2 - 20r - 3}{10r^2 + 1} = \frac{30a^2 - 20ab - 3b^2}{10a^2 + b^2}$$

so $x = 30a^2 - 20ab - 3b^2$, $z = 10a^2 + b^2$ and (by plugging into the equation for the line) $y = -(10a^2 + 6ab - b^2)$ provide solutions.