1. As a sort of converse to Wilson's theorem, show that if n is not a prime then $(n-1)!$ is not congruent to -1 mod n. More precisely, when $n > 4$ and n is not prime, show that n divides $(n-1)!$, so $(n-1)! \equiv 0 \bmod n$. What happens when $n = 4$?

Solution: If n factors as the product pq of two different numbers $p > 1$ and $q > 1$ then p and q will be among the factors of $(n-1)!$ and hence n will divide $(n-1)!$. The only nonprime numbers n that cannot be factored in this way are the numbers $n = p^2$ with p prime. If $p > 2$ then p and $2p$ will be among the factors of $(n-1)!$ since $2p < p^2 = n$ so again n will divide $(n-1)!$. The only remaining case is $n = 2^2 = 4$, and in this case $(n-1)! = 3! = 6 \equiv 2 \bmod 4$.

2. Determine the values of Δ for which there exists a quadratic form of discriminant Δ that represents 5, and also determine the discriminants Δ for which there does not exist a form representing 5.

Solution: The criterion for the existence of a form of discriminant Δ representing n is that Δ is a square mod $4n$, so for $n = 5$ the condition is that Δ is a square mod 20. The squares mod 20 are $0^2 = 0$, $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 9$, $(\pm4)^2 = 16$, $(\pm5)^2 = 25 \equiv 5$, $(\pm6)^2 = 36 \equiv 16$, $(\pm7)^2 = 49 \equiv 9$, $(\pm8)^2 = 64 \equiv 4$, $(\pm9)^2 = 81 \equiv 1$, and $10^2 = 100 \equiv 0$. So the discriminants for which 5 is represented are the $\Delta \equiv 0, 1, 4, 5, 9, 16 \bmod 20$. Discriminants are numbers congruent to 0 or 1 mod 4, so mod 20 this means $0, 1, 4, 5, 8, 9, 12, 13, 16, 17$. Thus the discriminants for which 5 is not represented are the $\Delta \equiv 8, 12, 13, 17 \bmod 20$.

3. Verify that the statement of quadratic reciprocity is true for the following pairs of primes (p, q): $(3,5)$, $(3,7)$, $(3,13)$, $(5,13)$, $(7,11)$, and $(13,17)$.

Solution: First we can make a list of the nonzero squares mod p for the primes p that we're interested in:

$p = 3$: 1

5: 1, 4

7: 1, 2, 4

11: 1, 3, 4, 5, 9

13: 1, 3, 4, 9, 10, 12

17: 1, 2, 4, 8, 9, 13, 15, 16

We use the Legendre symbol $\left(\frac{a}{p}\right)$ which is defined to be $\left(\frac{a}{p}\right) = +1$ if a is a square mod p and $\left(\frac{a}{p}\right) = -1$ if a is not a square mod p. Here p is an odd prime which does

not divide a. The law of quadratic reciprocity then says $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both congruent to 3 mod 4, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

For the first pair $(p,q) = (3,5)$ we see from our list above that 3 is not a square mod 5 and neither is 5 a square mod 3. Thus we have $\left(\frac{3}{5}\right) = -1$ and $\left(\frac{5}{3}\right) = -1$ so $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)$ which is what quadratic reciprocity predicts since we are not in the exceptional case that both p and q are 3 mod 4. Similarly in the other cases we have $\left(\frac{3}{7}\right) = -1 = -\left(\frac{7}{3}\right)$, $\left(\frac{3}{13}\right) = +1 = \left(\frac{13}{3}\right)$, $\left(\frac{5}{13}\right) = -1 = \left(\frac{13}{5}\right)$, $\left(\frac{7}{11}\right) = -1 = -\left(\frac{11}{7}\right)$, $\left(\frac{13}{17}\right) = +1 = \left(\frac{17}{13}\right)$. In each case we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless both p and q are congruent to 3 mod 4, in which case we have $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

4. (a) In the book there is an example near the end of section 2.3 working out which primes are represented by some form of discriminant 13, using quadratic reciprocity for the key step. (This was also done in class.) Do the same thing for discriminant 17.

Solution: The special primes that divide the discriminant are represented, so that is just 17 in this case. The prime 2 is represented since 17 is not congruent to 5 mod 8. For other odd primes p the criterion for representability is that 17 is a square mod p, so $\left(\frac{17}{p}\right) = +1$. In the previous problem we listed the squares mod 17, which were $1,2,4,8,9,13,15,16$. So the primes represented are 17 and the primes congruent to one of $1,2,4,8,9,13,15,16$ mod 17. Equivalently, we could say $\pm1, \pm2, \pm4, \pm8$ mod 17.

(b) Show that all forms of discriminant 17 are equivalent to the principal form $x^2 + xy - 4y^2$.

Solution:

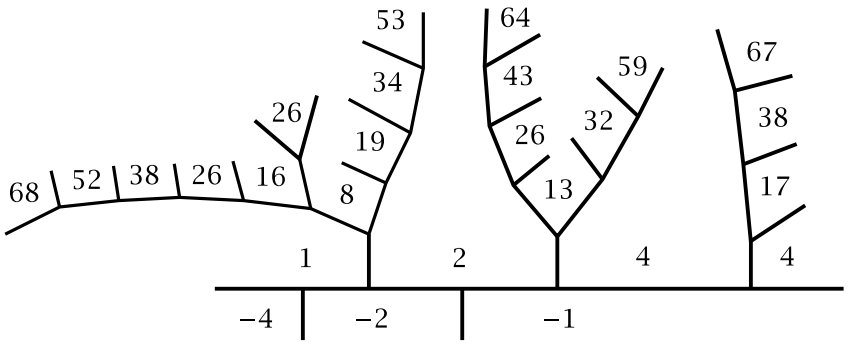
h	pq	(p,q)
1	4	$(1,4),\ (2,2),\ (4,1)$
3	2	$(1,2),\ (2,1)$

1	2	4	4	2	1
−4	−2	−1		−2	−4

All (p,q) are realized by $x^2 + xy - 4y^2$ so all forms with $\Delta = 17$ are equivalent.

(c) Draw enough of the topograph of $x^2 + xy - 4y^2$ to show all values between -70 and 70, and verify that the primes that occur are precisely the ones predicted by your answer in part (a).

Solution: The negative values are just the negatives of the positive values, so there is no need to show them all.



The primes that occur here are $2, 13, 17, 19, 43, 47, 53, 59, 67$. Excluding 17 itself, each of these primes is congruent to one of $1, 2, 4, 8, 9, 13, 15, 16 \bmod 17$, and every prime congruent to one of $1, 2, 4, 8, 9, 13, 15, 16 \bmod 17$ that is less than 70 is on this list.

5. Using quadratic reciprocity as in part (a) of the previous problem, figure out which primes are represented by at least one form of discriminant Δ for the following values of Δ: -3, 8, -20, 21.

Solution: For $\Delta = -3$ the special prime 3 is represented, but 2 is not represented since $-3 \equiv 5 \bmod 8$. For other primes p we have $\left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. This equals $(+1)[+\left(\frac{p}{3}\right)]$ when $p = 4k+1$ and it equals $(-1)[-\left(\frac{p}{3}\right)]$ when $p = 4k+3$ so it equals $\left(\frac{p}{3}\right)$ in all cases. The only nonzero square mod 3 is 1, so only the primes $p \equiv 1 \bmod 3$ are represented, in addition to the special prime 3.

For $\Delta = 8$ the special prime is 2 and this is represented. For odd primes p we have $\left(\frac{\Delta}{p}\right) = \left(\frac{8}{p}\right) = [\left(\frac{8}{p}\right)]^3 = \left(\frac{2}{p}\right)$ and this equals $+1$ only for $p \equiv \pm 1 \bmod 8$, so these are the primes that are represented, in addition to 2.

For $\Delta = -20$ the special primes 2 and 5 are represented. For the other primes p we have $\left(\frac{\Delta}{p}\right) = \left(\frac{-20}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$. We compute the values of this on congruence classes mod 20 that aren't divisible by the special primes 2 and 5 that divide 20. These are the classes $1, 3, 7, 9, 11, 13, 17, 19$, where the corresponding values of $\left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$ are $1 \to (+1)(+1)$, $3 \to (-1)(-1)$, $7 \to (-1)(-1)$, $9 \to (+1)(+1)$, $11 \to (-1)(+1)$, $13 \to (+1)(-1)$, $17 \to (+1)(-1)$, $19 \to (-1)(+1)$. Thus the primes represented are $p \equiv 1, 3, 7, 9 \bmod 20$, in addition to 2 and 5.

For $\Delta = 21$ the special primes 3 and 7 are represented, but 2 is not since $21 \equiv 5 \bmod 8$. For other primes p we have $\left(\frac{\Delta}{p}\right) = \left(\frac{21}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{7}{p}\right)$. This equals $\left(\frac{p}{3}\right)\left(\frac{7}{p}\right)$ since when we apply reciprocity to each of $\left(\frac{3}{p}\right)$ and $\left(\frac{7}{p}\right)$ we get two plus signs when

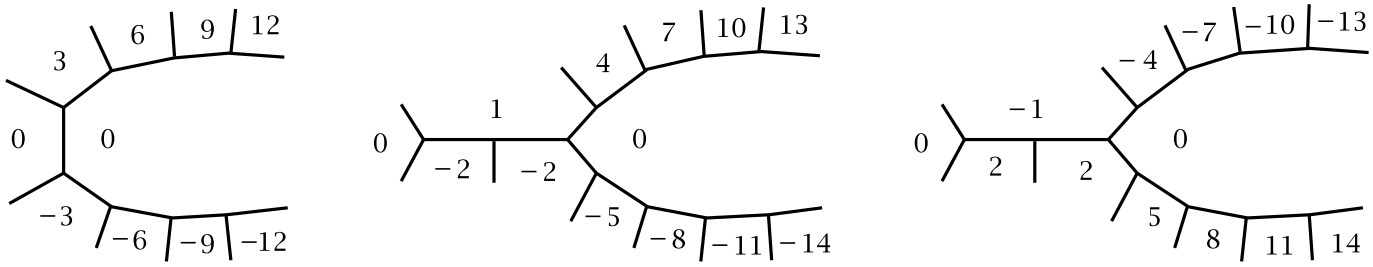
$p = 4k+1$ and two minus signs when $p = 4k+3$. We evaluate $\left(\frac{p}{3}\right)\left(\frac{7}{p}\right)$ in the cases $1,2,4,5,8,10,11,13,16,17,19,20$ and we get $1 \to (+1)(+1)$, $2 \to (-1)(+1)$, $4 \to (+1)(+1)$, $5 \to (-1)(-1)$, $8 \to (-1)(+1)$, $10 \to (+1)(-1)$, $11 \to (-1)(+1)$, $13 \to (+1)(-1)$, $16 \to (+1)(+1)$, $17 \to (-1)(-1)$, $19 \to (+1)(-1)$, $20 \to (-1)(-1)$. Thus the primes represented are $p \equiv 1,4,5,16,17,20 \bmod 21$, in addition to 3 and 7.

6. (a) Repeat the previous problem for $\Delta = 9$ where the answer may be rather surprising. Note that quadratic forms with $\Delta = 9$ are 0-hyperbolic, rather than the more usual hyperbolic or elliptic forms that we consider. (0-hyperbolic forms factor into linear factors with integer coefficients.)

Solution: The special prime 3 dividing Δ is represented, as is 2 since 9 is not congruent to $5 \bmod 8$. For other primes p we have $\left(\frac{\Delta}{p}\right) = \left(\frac{9}{p}\right) = \left[\left(\frac{3}{p}\right)\right]^2 = +1$. So all primes are represented.

(b) Draw enough of the topographs of all three equivalence classes of forms with $\Delta = 9$ to see why the answer you got in part (a) is correct.

Solution: One form with $\Delta = 9$ is $Q_1 = 3xy$, with two adjacent regions in its topograph that have labels 0. There are two forms that have a separator line, $Q_2 = x^2 + xy - 2y^2$ and $Q_3 = 2x^2 + xy - y^2$. Parts of the topographs for these three forms are shown below:



In the regions adjacent to the 0 regions we see that Q_1 takes all values congruent to $0 \bmod 3$, Q_2 takes all values congruent to $1 \bmod 3$, and Q_2 takes all values congruent to $2 \bmod 3$. Since every number is congruent to one of these three values mod 3, these forms together take on all integer values, and in particular all prime values.

(c) Show that in fact *every* integer n is represented primitively by at least one quadratic form of discriminant 9.

Solution: Answered in part (b).