HW 6 solutions

JC

April 11, 2003

1. (a) There are four rotations (counting the identity as a rotation through 0 degrees) and four reflections, two in the diagonals and two in the lines that join the midpoints of opposing edges.

   We label the rotations through 0, 90, 180 and 270 degrees (anticlockwise) as 0, 1, 2, 3 respectively. To label the reflections we think of the vertices as the points $(\pm 1, \pm 1)$. 4 is the reflection in $x + y = 0$, 5 is the reflection in $x = 0$, 6 is the reflection in $y = x$, 7 is the reflection in $y = 0$.

   (b) It is clear that the composition of any two symmetries of F is a symmetry of F, so composition is a binary operation on symmetries. Associativity is easy, symmetries are functions from the plane to itself and composition is associative on the class of all functions. The identity is a symmetry of F. Symmetries of the plane are bijections and the inverse of a symmetry of the plane is a symmetry of the plane: what is more if σ maps F to F then so does σ^{-1}.

   (c) Here is the table.

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	0	7	4	5	6
2	2	3	0	1	6	7	4	5
3	3	0	1	2	5	6	7	4
4	4	5	6	7	0	1	2	3
5	5	6	7	4	3	0	1	2
6	6	7	4	5	2	3	0	1
7	7	4	5	6	1	2	3	0

   A subtle point: the composition of f and g is g followed by f, so for example 1*4 is 4 followed by 1. The group is not commutative, for example 1*4 = 7, 4*1=5.

   (d) It is not hard to see that a nonempty subset of a group is a subgroup exactly when it is closed under the group operation and under inversion.

   Clearly $S_0 = \{0\}$ is a subgroup as is $S_1 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

If a subgroup contains 1 then it must contain 1*1 =2 and 1*2 =3. At this point we have closed off so $S_2 = \{0, 1, 2, 3\}$ is a subgroup. From the table any subgroup which contains S_2 and an element outside S_2 must be the whole group, so the only subgroups which contain 1 (or 3 by a similar argument) are S_1 and S_2.

Clearly $S_3 = \{0, 2\}$ is a subgroup. Similarly each of $S_4 = \{0, 4\}$, $S_5 = \{0, 5\}$, $S_6 = \{0, 6\}$ and $S_7 = \{0, 7\}$ is a subgroup.

Now look at subgroups containing 2 but not 1 or 3 (we already considered the ones which do have 1 or 3). 2*4 = 6, 2*6=4, 4*6=2 and so on and a little calculation shows that $S_8 = \{0, 2, 4, 6\}$ is a subgroup, and similarly $S_9 = \{0, 2, 5, 7\}$ is a subgroup. These are the only possibilities because for example $4 * 5 = 1$.

The product of any two elemnts from $\{4, 5, 6, 7\}$ is in $\{0, 1, 2, 3, \}$ so we have covered all possibilities. There are ten subgroups.

2. (a) Let $d = gcd(X, n)$ and $e = gcd(Y, n)$. Suppose $X - Y = An$. Then since d divides both X and n, d divides Y and so $d \leq e = gcd(Y, n)$. Similarly $e \leq d$ so $e = d$.

   (b) Compute $b = a^A \ mod \ n$ and then $gcd(b - 1, n)$. This works by the first part of the question. You cannot afford to compute a^A and then feed $a^A - 1$ into Euclid, because (among other reasons) Euclid will need on the order of $Aln_2(a)$ operations to compute the gcd and that is way too much.

   (c) If p divides both a and n then $p \leq gcd(a, n)$. If p does not divide a then by Fermat $a^{p-1} \equiv 1 mod\ p$, and since $p-1$ divides A we get $a^A \equiv 1\ mod\ p$. In this case p divides n and $a^A - 1$ so $p \leq gcd(a^A - 1, n)$.

   (d) See worksheet linked from the main web page.

   (e) You want to choose p so that $p - 1$ does not divide $k!$ for any k which your opponent could reasonably use. Now $k!$ is only divisible by primes up to k so your best bet is to make $p - 1$ have a large prime factor, and the hardest case for your opponent will be when $(p - 1)/2$ is prime. Similarly for q.

   As we see on the worksheet, primes are so common that we can quickly find such p and q.

   [Alternative: find p and q so that both $p - 1$ and $q - 1$ divide $k!$ for some smallish k]