Torsdag, v.4

5. Notera att $122 \equiv 2 \pmod 8$. Som vi såg på föreläsningen i morse (måndag, v.5), om a är ett godtyckligt heltal så gäller att

$$a^2 \equiv 0, 1 \text{ eller } 4 \pmod 8.$$

Nu ska man kontrollera att uttrycket $x^2 - 5y^2$ inte kan anta något värde som är $\equiv 2 \pmod 8$ (och inte heller 6 (mod 8) förresten). Det är bara att kolla alla möjligheterna, som vi gör i tabellen nedan :

$x^2 \pmod 8$	$y^2 \pmod 8$	$x^2 - 5y^2 \pmod 8$
0	0	$0 - 5 \cdot 0 = 0$
1	0	$1 - 5 \cdot 0 = 1$
4	0	$4 - 5 \cdot 0 = 4$
0	1	$0 - 5 \cdot 1 = -5 \equiv 3$
1	1	$1 - 5 \cdot 1 = -4 \equiv 4$
4	1	$4 - 5 \cdot 1 = -1 \equiv 7$
0	4	$0 - 5 \cdot 4 = -20 \equiv 4$
1	4	$1 - 5 \cdot 4 = -19 \equiv 5$
4	4	$4 - 5 \cdot 4 = -16 \equiv 0$

Tisdag, v.5

4. $\mathbf{Z}$ is a domain : we all know that if the product of two integers is zero then one of them must itself be zero. $\mathbf{Z}_{36}$ is not a domain since, for example,

$$9 \cdot 4 \equiv 0 \pmod{36},$$

but neither 9 nor 4 is itself a multiple of 36. On the other hand, $\mathbf{Z}_{37}$ is a domain, since 37 is a prime. More generally, the point is that the following holds (see Theorems 14.7 and 14.8 in Grimaldi) :

Proposition *Let R be a finite (i.e.: as a set, R contains finitely many elements) commutative ring with unity. Then R is an integral domain if and only if R is a field.*

Proof : First suppose R is a field. Let a, b be two elements of R and

suppose $a \cdot b = 0$. We must show that either $a = 0$ or $b = 0$. Suppose $a \neq 0$. Then a^{-1} exists, since R is a field. Thus

$$a \cdot b = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

But, by associativity of multiplication in R, we have that $a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b$. Hence $b = 0$, as required.

Now suppose instead that R is an integral domain. Let a be any non-zero element of R. We must show that there exists $b \in R$ such that $a \cdot b = 1$. Suppose that R has $n+1$ elements in total and list them as $r_0, r_1, ..., r_n$ such that $r_0 = 0$ and $r_1 = a$. Now, since R is a domain, each of the products

$$r_1 \cdot r_j, \quad j = 1, ..., n,$$

is a non-zero element of R. I claim further that all these products are distinct elements of R. For suppose $r_1 \cdot r_i = r_1 \cdot r_j$. Thus, by the distributive law, $0 = r_1 \cdot r_i - r_1 \cdot r_j = r_1 \cdot (r_i - r_j)$. But now, since R is a domain and since $r_1 \neq 0$, we must have that $r_i - r_j = 0$, hence $i = j$.

This establishes our claim. Now the point is that we have n distinct non-zero elements $r_1 \cdot r_j$ of R, but that is just the total number of non-zero elements of R, hence one of these products must equal 1, thus proving that $r_1 = a$ has an inverse, v.s.v.

Tisdag v.6

2(ii) In Monday's lecture, we already established the result when $\mathrm{GCD}(a, n) = 1$, using Euler's theorem. There are three remaining cases, depending on whether $\mathrm{GCD}(a, n) = p, q$ or n itself. In fact, the first two of these are identical by symmetry. The third is trivial, because then $a \equiv 0 \pmod{n}$, so the same is obviosuly true for any power of a.

So, without loss of generality, it remains to establish the result when $\mathrm{GCD}(a, n) = p$. We must show that $a^k \equiv a \pmod{n}$, i.e.: that n divides $a^k - a$. It suffices to show that $a^k - a$ is divisible by both p and q, i.e.: to show that

$$a^k \equiv a \pmod{p}, \tag{1}$$
$$a^k \equiv a \pmod{q}. \tag{2}$$

Now (1) is trivial, since by hypothesis p divides a, so that both sides are congruent to zero modulo p. For (2) we use the fact that $n = pq \Rightarrow \phi(n) = (p-1)(q-1)$, hence $q-1$ divides $\phi(n)$, from which it follows that since $k \equiv 1 \pmod{\phi(n)}$ then $k \equiv 1 \pmod{q-1}$ also. That is, $k = 1 + m \cdot (q-1)$ for some integer m. By Fermat's theorem, since q does not divide a, we have that

$$a^{q-1} \equiv 1 \pmod{q}.$$

But then

$$a^k = a^1 \cdot (a^{q-1})^m \equiv a \cdot 1^m \equiv a \pmod{q}, \quad \text{v.s.v.}$$

4. Suppose G is not connected, so that G contains at least two connected components. Let v, w be any two vertices in G. We need to show that there is a path from v to w in $\overline{G}$. If v and w lie in different connected components of G, then there is an EDGE between them in $\overline{G}$, so that's ok. If they're in the same component of G, then let z be any vertex in some other component. There are edges from both v and w to z in $\overline{G}$ and hence a 2-edge path from v to w via z.

This completes the proof. Note that we've shown that, not only is either G or $\overline{G}$ connected but that if G is disconnected, then not only is $\overline{G}$ connected, but each pair of vertices can be joined by a path of length at most two in it.