

Two proofs of number 49, chapter 8

The light at the end of the tunnel

March 11, 2008



Here are two proofs of number 49, one that involves the book's hint, one that does not.
ROCK ON!

Chapter 8, Number 49: Let p be prime. How many subgroups of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ are there of order p ?

Solution 1: If H is a subgroup of order p , then it must be cyclic since p is prime. Consider the following collection of $p + 1$ distinct subgroups, let $k = 1, 2, \dots, p - 1$:

$$H_k = \langle (1, k) \rangle, \quad H_0 = \langle (0, 1) \rangle.$$

Each of these is a cyclic subgroup of order p , and we prove presently that each of these are distinct.

H_0 is distinct from each of the H_k , since $\ell(1, k) = (\ell, \ell k) = (0, 1)$ only if $p|\ell$, in which case $\ell k = 0 \neq 1$ in \mathbb{Z}_p . In very much the same spirit, $H_k \neq H_j$ for $k \neq j$. For suppose that $\ell(1, k) = (1, j)$. Then $\ell = 1$ (or any number $1 \pmod p$), and thus $k = j$, a contradiction to $k \neq j$.

We claim that these are the only subgroups of order p . Let H be a subgroup of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Then H is cyclic, and $H = \langle (a, b) \rangle$. There are two possibilities: $a = 0$ or $a \neq 0$.

If $a = 0$, then $(0, b) \in H_0$, and since every nonzero element of every group of prime order p is a generator for that group, $\langle (0, b) \rangle = H_0$.

If $a \neq 0$, then there exists a multiplicative inverse $u \in \mathbb{Z}_p$. Then $u(a, b) = (ua, ub) = (1, ub) \in H_{ub}$. Again, this nonzero element must be a generator for this group, and in this

case $H = H_k$ for some k .

Solution 2: There are $p^2 - 1$ elements of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$, since every nonzero element has order p , and there are $p^2 - 1$ such elements. Moreover, every element of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ generates a subgroup of order p . Let H be a subgroup of order p . Then there are $p - 1$ elements of order p . If K is another subgroup of order p , then $H \cap K \leq H$, and so by Lagrange's theorem, $H \cap K$ has order 1 or p . So if $K \neq H$, then $H \cap K$ contains only the identity.

So we count the elements of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ as follows. For any nonidentity element (a, b) , we construct the cyclic group $\langle (a, b) \rangle$ of order p , accounting for p elements of $\mathbb{Z}_p \oplus \mathbb{Z}_p$. We consider any (nonidentity) element outside of that subgroup, and construct its cyclic subgroup. It is important to note that you account for exactly $p - 1$ elements of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ by doing this. There are $p + p$ elements in both subgroups combined, but since they're not equal, the only element which was counted twice was the identity. Thus each addition of a new subgroup of order p accounts for $p - 1$ more elements of the group. Thus if k is the number of times we need to continue this process before we exhaust all elements of $\mathbb{Z}_p \oplus \mathbb{Z}_p$, then $p^2 = p + (k - 1)(p - 1)$, which has the solution $p = k + 1$. We claim that there could be no more distinct subgroups.

Let S be a subgroup of order p that is not one of the ones listed in the process above. There are $p \geq 2$ elements of S , then, and so there is a nonidentity element $(x, y) \in S$, and so this element must be an element of one of the subgroups K that we just constructed. But since $S \cap K$ has at least 2 elements in common, $S = K$.