COUNTING SUBGROUPS OF $\mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z}$

KEITH CONRAD

Fix a prime p. For nonnegative integers a, b, and d, we seek a formula for the number of subgroups of order p^d in $\mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z}$. Set

$$N_{a,b,d} = \#\{H \subset \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z} : \#H = p^d\}.$$

This is symmetric in a and b ($N_{a,b,d} = N_{b,a,d}$), so when it is convenient we can limit attention to the case $a \leq b$. Trivially $N_{a,b,d} = 0$ if $d > a + b$, so we may assume $0 \leq d \leq a + b$. For $1 \leq a \leq b$, and $a + b \geq d$, we will see that

$$N_{a,b,d} = 1 + p + p^2 + \cdots + p^r,$$

where $r = r(a, b)$ is a somewhat irregular function of a and b (the precise rule is given in Theorem 3).

Throughout, we write

$$G_{a,b} = \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z}.$$

For any abelian group G, its m-torsion subgroup will be denoted $G[m] = \{g \in G : g^m = e\}$.

We will develop a recursive formula for $N_{a,b,d}$ that requires knowing in advance how many cyclic subgroups there are of each size in $\mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z}$. So first we work out a formula for the number of cyclic subgroups. Write it as

$$C_{a,b,d} = \#\{H \subset \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z} : \#H = p^d, H \text{ is cyclic}\}.$$

Theorem 1. *When* $1 \leq a \leq b$,

$$C_{a,b,d} = \begin{cases} 1, & \text{if } d = 0, \\ p^{d-1} + p^d, & \text{if } 1 \leq d \leq a, \\ p^a, & \text{if } a + 1 \leq d \leq b \quad (\text{if } a \neq b), \\ 0, & \text{if } b < d. \end{cases}$$

In particular, $C_{a,b,1} = 1 + p$.

Proof. The cases $d = 0$ and $d > b$ are clear. So we may assume $1 \leq d \leq b$. To count subgroups of order p^d we count elements of order p^d and then divide by $\varphi(p^d)$ (the number of generators a cyclic group of order p^d has). An element has order p^d when it's killed by p^d but not by p^{d-1}, so

$$C_{a,b,d} = \frac{\#G_{a,b}[p^d] - \#G_{a,b}[p^{d-1}]}{\varphi(p^d)}.$$

How large is $G_{a,b}[p^i]$? If $0 \leq i \leq a$,

$$G_{a,b}[p^i] = p^{a-i}\mathbf{Z}/p^a\mathbf{Z} \times p^{b-i}\mathbf{Z}/p^b\mathbf{Z} \Longrightarrow \text{ size is } p^{2i}.$$

If $a \leq i \leq b$,

$$G_{a,b}[p^i] = \mathbf{Z}/p^a\mathbf{Z} \times p^{b-i}\mathbf{Z}/p^b\mathbf{Z} \Longrightarrow \text{ size is } p^{a+i}.$$

If $i > b$,

$$G_{a,b}[p^i] = \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^b\mathbf{Z} \Longrightarrow \text{ size is } p^{a+b}.$$

Putting this all together,

$$\#G_{a,b}[p^i] = \begin{cases} p^{2i}, & \text{if } 0 \leq i \leq a, \\ p^{a+i}, & \text{if } a \leq i \leq b, \\ p^{a+b}, & \text{if } i \geq b. \end{cases}$$

(The overlapping cases are consistent at $i = a$ and $i = b$.)

Now we feed the above formula for $\#G_{a,b}[p^i]$ at $i = d$ and $i = d-1$ into the formula for $C_{a,b,d}$. If $1 \leq d \leq a$,

$$C_{a,b,d} = \frac{p^{2d} - p^{2(d-1)}}{p^{d-1}(p-1)} = \frac{p^{2d-2}(p^2-1)}{p^{d-1}(p-1)} = p^{d-1}(p+1) = p^{d-1} + p^d.$$

If $a < b$ and $a + 1 \leq d \leq b$,

$$C_{a,b,d} = \frac{p^{a+d} - p^{a+d-1}}{p^{d-1}(p-1)} = \frac{p^{a+d-1}(p-1)}{p^{d-1}(p-1)} = p^a.$$

□

Theorem 2. *For $1 \leq a \leq b$, we have*

$$N_{a,b,0} = 1$$

and

$$N_{a,b,1} = C_{a,b,1} = 1 + p.$$

If $d \geq 2$ then

$$N_{a,b,d} = C_{a,b,d} + N_{a-1,b-1,d-2}.$$

Proof. A group of order p is cyclic, so

$$N_{a,b,1} = C_{a,b,1} = 1 + p.$$

Now take $d \geq 2$. We can distinguish cyclic from noncyclic subgroups of $G_{a,b}$ using p-torsion. The p-torsion in $G_{a,b}$ is

$$G_{a,b}[p] = p^{a-1}\mathbf{Z}/p^a\mathbf{Z} \times p^{b-1}\mathbf{Z}/p^b\mathbf{Z},$$

which has order p^2, so

$$G_{a.b}/G_{a,b}[p] \cong \mathbf{Z}/p^{a-1}\mathbf{Z} \times \mathbf{Z}/p^{b-1}\mathbf{Z} \cong G_{a-1,b-1}.$$

For any nontrivial subgroup $H \subset G_{a,b}$, if H is cyclic then $H[p]$ has order p, while if H is noncyclic then $H \cong \mathbf{Z}/p^j\mathbf{Z} \times \mathbf{Z}/p^k\mathbf{Z}$ for some positive integers j and k, so $H[p]$ has order p^2. Since $H[p] \subset G_{a,b}[p]$ and $G_{a,b}[p]$ has order p^2, $H[p] = G_{a,b}[p]$. So

$$H \text{ not cyclic } \Longrightarrow G_{a,b}[p] \subset H \subset G_{a,b}.$$

The converse is true as well, since $G_{a,b}[p] \cong (\mathbf{Z}/p\mathbf{Z})^2$ contains more than one subgroup of order p, so it can't lie inside a cyclic group. So for $2 \leq d \leq a + b$,

$$\begin{aligned} \#\{H \subset G_{a,b} : \#H = p^d, H \text{ not cyclic}\} &= \#\{\overline{H} \subset G_{a,b}/G_{a,b}[p] : \#\overline{H} = p^{d-2}\} \\ &= N_{a-1,b-1,d-2}, \end{aligned}$$

which leads to a recursive formula: $N_{a,b,d}$ is the number of cyclic subgroups of $G_{a,b}$ with order p^d (which is $C_{a,b,d}$) plus the number of noncyclic subgroups of $G_{a,b}$ with order p^d (which we just showed is $N_{a-1,b-1,d-2}$ if $d \geq 2$). □

Using Theorems 1 and 2 (and sometimes the equation $N_{a,b,d} = N_{a,b,a+b-d}$, which follows from duality theory for finite abelian groups), the following formulas for $N_{a,b,d}$ are found when $1 \le a \le b$ and $1 \le d \le 5$:

$$N_{a,b,1} = 1 + p,$$

$$N_{a,b,2} = \begin{cases} 1, & \text{if } a = b = 1, \\ 1 + p, & \text{if } a = 1, b \ge 2, \\ 1 + p + p^2, & \text{if } a \ge 2, \end{cases}$$

$$N_{a,b,3} = \begin{cases} 1, & \text{if } a = 1, b = 2, \\ 1 + p, & \text{if } a = 1, b \ge 3; a = 2, b = 2, \\ 1 + p + p^2, & \text{if } a = 2, b \ge 3, \\ 1 + p + p^2 + p^3, & \text{if } a \ge 3, \end{cases}$$

$$N_{a,b,4} = \begin{cases} 1, & \text{if } a = 1, b = 3; a = 2, b = 2, \\ 1 + p, & \text{if } a = 1, b \ge 4; a = 2, b = 3, \\ 1 + p + p^2, & \text{if } a = 2, b \ge 4; a = 3, b = 3, \\ 1 + p + p^2 + p^3, & \text{if } a = 3, b \ge 4, \\ 1 + p + p^2 + p^3 + p^4, & \text{if } a \ge 4, \end{cases}$$

and

$$N_{a,b,5} = \begin{cases} 1, & \text{if } a = 1, b = 4; a = 2, b = 3, \\ 1 + p, & \text{if } a = 1, b \ge 5; a = 2, b = 4; a = 3, b = 3, \\ 1 + p + p^2, & \text{if } a = 2, b \ge 5; a = 3, b = 4, \\ 1 + p + p^2 + p^3, & \text{if } a = 3, b \ge 5; a = 4, b = 4, \\ 1 + p + p^2 + p^3 + p^4, & \text{if } a = 4, b \ge 5, \\ 1 + p + p^2 + p^3 + p^4 + p^5, & \text{if } a \ge 5. \end{cases}$$

Examine these according to the constraints on a and b for each formula for $N_{a,b,d}$. The pattern of cases where inequalities on b appear is obvious: $a = 1, b \ge d$, then $a = 2, b \ge d$, then $a = 3, b \ge d$, and so on as a increases up to $d - 1$. The remaining cases where a and b both have specified values are organized according to increasing values of $a + b$ for $1 \le a \le b \le d - 1$. We are led to the following general theorem.

Theorem 3. *If $1 \le a \le b$, then*

$$N_{a,b,d} = \begin{cases} 1 + p + \cdots + p^d, & \text{if } 0 \le d \le a, \\ 1 + p + \cdots + p^a, & \text{if } a \le d \le b, \\ 1 + p + \cdots + p^{a+b-d}, & \text{if } b \le d \le a + b, \\ 0, & \text{if } a + b < d. \end{cases}$$

Therefore when $0 \le d \le a + b$, $N_{a,b,d} = 1 + p + \cdots + p^r$ where $0 \le r \le d$.

Proof. Use induction on b. □

Example 4. When $a = b$,

$$N_{a,a,d} = \begin{cases} 1 + p + \cdots + p^d, & \text{if } 0 \le d \le a, \\ 1 + p + \cdots + p^{2a-d}, & \text{if } a \le d \le 2a. \end{cases}$$

Theorem 3 says that as d increases from 0 to $a+b$, $N_{a,b,d}$ starts out as $1, 1+p, 1+p+p^2, \dots,$ increasing by the next power of p each time until reaching $1+p+\cdots+p^a$ at $d=a$. Then $N_{a,b,d}$ stays at this value until d reaches b, after which the highest power of p is removed for each successive value of d until $N_{a,b,d}$ reaches $N_{a,b,a+b}=1$.

Corollary 5. *Suppose* $1 \leq a \leq b$.

1. *If* $1 \leq d \leq a$ *then* $N_{a,b,d} = N_{a,b,d-1} + p^d$.
2. *If* $a < d \leq b$ *then* $N_{a,b,d} = N_{a,b,d-1}$.
3. *If* $b < d \leq a+b$ *then* $N_{a,b,d} = N_{a,b,d-1} - p^{a+b-d+1}$.

In particular, $N_{a,b,d} \equiv N_{a,b,d-1} \bmod p^d$ *if* $1 \leq d \leq b$ *but not necessarily if* $b < d \leq a+b$.

Proof. From the description of how $N_{a,b,d}$ rises, plateaus, and then falls, this is obvious. □

For each a, b, and d, observe that $N_{a,b,d}$ has the same formula for all p. So $N_{a,b,d}$ can be described by a "universal" formula for all primes. More generally, if A is a finite abelian p-group that is a product of cyclic groups of orders $p^{e_1}, \dots, p^{e_r}$ ($e_i > 0$), then the number of subgroups of A with a particular order p^d is a universal polynomial function of p (same formula for all p) that is determined by d and the exponents e_i. Even more generally, the number of subgroups H of A such that H and A/H have specified cyclic decompositions is given by a universal polynomial in p that is determined by the sizes of the cyclic components of H, A/H, and A; these universal polynomials in p are called *Hall polynomials*. There is also a formula, due to Delsarte, for the number of subgroups of A with a given isomorphism type. See [1] and [2].

References

[1] G. Constantine and R. S. Kulkarni, "On a result of S. Delsarte," *Proc. Amer. Math. Soc.* **92** (1984), 149–152.

[2] S. Delsarte, "Fonctions de Möbius sur les groupes abliens finis," *Annals of Math.* **49** (1948), 600–609.