1 Cyclic group of order n

is, effectively, the set $\mathbb{Z}_n$ under addition $\bmod n$. It is isomorphic to

$$\mathbf{p}_1^{\mathbf{k}_1} \oplus \mathbf{p}_2^{\mathbf{k}_2} \oplus ... \oplus \mathbf{p}_\ell^{\mathbf{k}_\ell} \tag{1}$$

where $\mathbf{p}^{\mathbf{k}}$ is our notation for cyclic group of order p^k, and $p_1^{k_1} p_2^{k_2} ... p_\ell^{k_\ell}$ is the prime decomposion of n.

The isomorphism is a 'natural' one, i.e. when $j \in \mathbb{Z}_n$, the corresponding element of (1) is

$$\left(j \bmod p_1^{k_1}, j \bmod p_2^{k_2}, ..., j \bmod p_\ell^{k_\ell} \right)$$

EXAMPLE: When $n = 72 = 2^3 \times 3^2$, the nubers 31 and 53 are represented by $(7, 4)$ and $(5, 8)$ respectively. Adding the last two $\bmod (2^3, 3^2)$ yields $(4, 3)$, which corresponds to the correct answer of 12 (Maple's 'isolve' can help you find it).■

It is obvious that $\mathbf{p}^{\mathbf{k}}$ has $p^k - p^{k-1}$ elements of order p^k, $p^{k-1} - p^{k-2}$ elements of order p^{k-1}, ..., $p - 1$ elements of order p, and one element of order 1, and it is also clear what these are (not divisible by p, divisible by p but not p^2, ... etc.).

Similarly, we can tell what is the order of any element of (1), and how many elements of each order they are (as the orders of individual components simply multiply).

2 Abelian groups of order n

are not all of the above type. In the simplest case of $n = p^K$, there are 'numbpart(K)' number of possiblities, from $\mathbf{p}^{\mathbf{K}}$ to $\mathbf{p} \oplus \mathbf{p} \oplus ... \oplus \mathbf{p}$ (K of these). Taking any one of these, say

$$\mathbf{p}^{\mathbf{k}_1} \oplus \mathbf{p}^{\mathbf{k}_2} \oplus ... \oplus \mathbf{p}^{\mathbf{k}_\ell}$$

where $k_1 \geq k_2 \geq ... \geq k_\ell$ we can see that the largest possible order of an element is p^{k_1}, and that this will be achieved by making the first component *not* divisible by p (the other components can be arbitrary). When $k_2 = k_1$, this can be also achived by making the *second* component not divisible by p. and the rest arbitrary, etc.

So, in general, when $k_1 = k_2 = ... = k_m$, there are

$$n \left(1 - \frac{1}{p^m} \right)$$

such maximum-order elements, where $n = p^K$.

When different primes are involved, we just multiply these.

EXAMPLE: The group

$$\mathbf{2}^{\mathbf{3}} \oplus \mathbf{2}^{\mathbf{3}} \oplus \mathbf{2} \oplus \mathbf{5}^{\mathbf{4}} \oplus \mathbf{5}^{\mathbf{3}}$$

has $2^7(1 - \frac{1}{2^2}) \times 5^7(1 - \frac{1}{5}) = 6,000,000$ elements of order $2^3 \times 5^4 = 5000$. These can be found by making the first *or* the second component *not* divisible by 2, and the fourth component no divisible by 5 (the remaining components can be arbitrary).■

3 Multiplicative group $\mathrm{mod}\ n$

consists of all elements of $\mathbb{Z}_n$ which are relatively prime to n (i.e. when $n = p_0^{k_0} p_1^{k_1} ... p_\ell^{k_\ell}$, they are not divisible by $p_0, p_1, ..., p_\ell$). We will denote this group by $\boxed{n}$. One can show that this group is isomorphic to

$$\boxed{p_0^{k_0}} \otimes \boxed{p_1^{k_1}} \otimes ... \otimes \boxed{p_\ell^{k_\ell}} \tag{2}$$

under the same 'natural' isomorphism as before. Clearly, the size of $\boxed{p^k}$ is $p^k - p^{k-1} = (p-1)p^{k-1}$, so the size of the whole $\boxed{n}$ group is $(p_0-1)p_0^{k_0-1}(p_1-1)p_1^{k_1-1}...(p_\ell-1)p_\ell^{k_\ell-1}$.

EXAMPLE: When $n = 72$, multiplying 31 and 53 results, in the $(7,4)$ and $(5,8)$ representation, in $(3,5)$, which corresponds to the correct answer of 51.

Now comes the main point: as an Abelian group, $\boxed{p^k}$ must be also isomorphic to one of the groups of the previous section (of the same size). Luckily, it happens to be

$$(\mathbf{p-1}) \oplus \mathbf{p^{k-1}}$$

when $p \neq 2$ and

$$\mathbf{2} \oplus \mathbf{2^{k-2}}$$

when $p = 2$. The exact isomorphism is now more complicated (it clearly cannot be of a 'natural' type).

From now on thus becomes convenient to use the following notation for the prime decomposition of n

$$n = 2^{k_0} p_1^{k_1} p_2^{k_2} ... p_\ell^{k_\ell}$$

In conclusion, the corresponding group $\boxed{n}$ is isomorphic to

$$\mathbf{2} \oplus \mathbf{2^{k_0-2}} \oplus (\mathbf{p_1-1}) \oplus \mathbf{p^{k_1-1}} \oplus (\mathbf{p_2-1}) \oplus \mathbf{p^{k_2-1}} \oplus ... \oplus (\mathbf{p_\ell-1}) \oplus \mathbf{p^{k_\ell-1}}$$

where each of the $(\mathbf{p-1})$ components can and should be further decomposed.

EXAMPLE: $\boxed{9000}$ is isomorphic (based on $9000 = 2^3 3^2 5^3$) to

$$(\mathbf{2} \oplus \mathbf{2}) \oplus (\mathbf{2} \oplus \mathbf{3}) \oplus \left(\mathbf{4} \oplus \mathbf{5^2}\right)$$

or

$$\mathbf{2^2} \oplus \mathbf{2} \oplus \mathbf{2} \oplus \mathbf{2} \oplus \mathbf{3} \oplus \mathbf{5^2}$$

The maximum order of an element is $2^2 \times 3 \times 5^2 = 300$, and there is $2^5(1-\frac{1}{2}) \times 3(1-\frac{1}{3}) \times 5^2(1-\frac{1}{5}) = 640$ of these. In the additive representation, it is easy to tell what they are, but that does not tell us how to find them in the original $\boxed{9000}$.■

In general, we have to figure it out for each $\boxed{p^k}$ individually and then, using (2), to put everything together.

Let's try to do this, first for the simplest case of 3^k:

When $k = 1$

#	period
1	1
2	2

When $k = 2$

#	period
1	1
$1 + 3 = 4,\ 1 + 6 = 7$	3
$2 + 6 = 8$	2
$2,\ 2 + 3 = 5$	6

When $k = 3$

#	period
1	1
$1 + 9 = 10,\ 1 + 18 = 19$	3
$4,\ 4 + 9 + 13,\ 4 + 18 = 22$ $7,\ 7 + 9 = 16,\ 7 + 18 = 25$	9
$8 + 18 = 26$	2
$8,\ 8 + 9 = 17$	6
$2,\ 2 + 9 = 11,\ 2 + 18 = 20$ $5,\ 5 + 9 = 14,\ 5 + 18 = 23$	18

Starting from $k = 2$, the last row (of full-period elements) always consists of all numbers whose $\bmod\ 9$ equals 2 or 5. If we are happy with half the full period, we would take numbers whose $\bmod 9$ equals 4 or 7, one third of the full period requires $\bmod 9$ equal to 8.

Similarly, for 5^k we get:

When $k = 1$

#	period
1	1
4	2
$2,\ 3$	4

When $k = 2$

#	period
1	1
$1 + 5 = 6,\ 1 + 10 = 11,\ 1 + 15 = 16, 1 + 20 = 21$	5
$4 + 20 = 24$	2
$4,\ 4 + 5 = 9,\ 4 + 10 = 14,\ 4 + 15 = 19$	10
$2 + 5 = 7,\ 3 + 15 = 18$	4
$2,\ 2 + 10 = 12,\ 2 + 15 = 17,\ 2 + 20 = 22$ $3,\ 3 + 5 = 8,\ 3 + 10 = 13,\ 3 + 20 = 23$	20

This implies that 2, 3, 8, 12, 13, 17, 22, 23 $\bmod 25$ will always yield the full period (for any $k \geq 2$), $4, 9, 14, 19 \bmod 25$ yield half a full period, and $6, 11, 16, 21 \bmod 25$ yield one quarter of a full period.

And, finally, the 'exceptional' case of 2^k:

When $k = 1$

#	period
1	1

When $k = 2$

#	period
1	1
$1 + 2 = 3$	2

When $k = 3$

#	period
1	1
$1 + 4 = 5,\ 3, 3 + 4 = 7$	2

When $k = 4$

#	period
1	1
$1 + 8 = 9,\ 7, 7 + 8 = 15$	2
$3,\ 5,\ 3 + 8 = 11,\ 5 + 8 = 13$	4

and it is from this point onwards ($k \geq 4$) that all numbers whose $\mathrm{mod}\ 8$ equals 3 or 5 yield the full period. (Half-full period would require one more step, resulting in $7, 9 \bmod 16$).