Subgroups of $Z$ and $\gcd$

Recall $Z$ is the set of integers, positive, negative and zero.

**Theorem:** The only subgroups of $(Z, +)$ are $\{0\}$, and $nZ$ for $n \geq 2$. (This includes the case $n = 1$, $Z$ itself.)

**Proof:** Let $H \neq \{0\}$ be a subgroup. Then $H$ contains some positive integer, since take any $x \in H$ with $x \neq 0$ and if it itself is not positive then $-x \in H$ and $-x$ is positive. Let $n$ be the least positive integer in $H$. As $H$ is closed under addition $2n = n + n, 3n = 2n + n, \ldots$ are in $H$ as well as their negatives so that $nZ \subseteq H$. (When $n = 1$ we already have $H = Z$ so let henceforth assume $n \geq 2$.)

**Claim:** $H = nZ$. Let $x \in H$. By division ($q, r$ stand for quotient and remainder respectively) write

$$x = nq + r \text{ with } 0 \leq r < n$$

As $nq \in H$ and $x \in H$ by closure $r \in H$. But as $n$ is the least positive integer in $H$ it must be that $r = 0$. So $x \in nZ$ giving the Claim, and hence the Theorem.

Now let $m, n \in Z - \{0\}$. Define

$$H = \{mx + ny : x, y \in Z\}$$

As $H$ is a group (exercise!!) and $H \neq \{0\}$ (e.g., $m \in H$) we have $H = dZ$. Thus

1. $d|m$ (since $m \in H = dZ$)
2. $d|n$ (since $n \in H = dZ$)
3. $d = mx + ny$ for some $x, y \in Z$ (since $d \in H$)

So $d$ is a common divisor of $m$ and $n$. But further let $e$ be any other common divisor. That is, suppose $e|m$ and $e|n$. Then we must have $e|mx$ and $e|ny$ so that $e|(mx + ny) = d$. That is, all other common divisors of $m, n$ divide $d$ and so in particular they are smaller than $d$.

**Definition:** We call $d$ the greatest common divisor of $m, n$ and write $d = \gcd(m, n)$.

**Definition:** When $\gcd(m, n) = 1$ we say that $m, n$ are relatively prime.

Note a nontrivial result.

**Corollary:** When $m, n$ are relatively prime there exist $x, y \in Z$ with $mx + ny = 1$. 


317 is a prime, not because we think so, or because our minds are shaped in one way rather than another, but *because it is so*, because mathematical reality is built that way.

– G.H. Hardy