Theorem 2.3.3, i.e., $c|d$ and consequently, d is the greatest common divisor. This completes the proof.

For example, $\gcd(-4, 20) = 4$ and $4 = (-4)\cdot(-1) + 20\cdot 0$

$\gcd(55, 35) = 5$ and $5 = 55\cdot 2 + 35\cdot(-3)$

$\gcd(0, 9) = 9$ and $9 = 0\cdot 0 + 9\cdot 1$

$\gcd(-9, 13) = 1$ and $1 = (-9)\cdot(-3) + 13\cdot(-2)$

Note 1 The $\gcd(a,b)$ is the least positive value of $ax + by$ where x and y are integers. (By the previous theorem)

But x and y are not uniquely determined integers for which the integer $ax + by$ is least positive. Because if $d = au + bv$, where u and v are integers then d can also be expressed as $d = a(u + bk) + b(v - ak)$ where k is an integer.

For example, let $a = 15$, $b = 24$. Then $d = 3$ and

$d = 15(-3) + 24\cdot 2$ which can also be expressed as

$d = 15(-3 + 24k) + 24(2 - 15k)$ where k is an integer

So, $3 = 15(-3) + 24\cdot 2 = 15(21) + 24(-13) = 15(-27) + 24(17)$

taking $k = 1$ and -1 etc.

Note 2 Guaranteed by the theorem it is always possible to express $\gcd(a,b)$ as $au + bv$. But the theorem gives no clue how to get u and v. We will see afterward that we will get a method to find at least one u and v.

Worked Examples (continued)

3. Show that $\gcd(a, a+2) = 1$ or 2 for every integer a.

Solution: Let $d = \gcd(a, a+2)$. Then $d \mid a$ and $d \mid a+2$

So, $d \mid ax + (a+2)y$ for all integers x, y.

Taking $x = -1$, $y = 1$, it follows that $d \mid 2$. So d is either 1 or 2

Theorem 2.3.7 If k be a positive integer, then for any integers a and b, not both zero, $\gcd(ka, kb) = k \cdot \gcd(a, b)$

Proof: Let $d = \gcd(a, b)$. Then there exists integers u and v such that $d = au + bv$. Since $\gcd(a, b) = d$,

$d \mid a$ and $d \mid b \Rightarrow kd \mid ka$ and $kd \mid kb$

So, kd is a common divisor of ka and kb

Let c be a common divisor of ka and kb

$c \mid ka \Rightarrow ka = pc$ for some integer p; and $c \mid kb$

$\Rightarrow kb = qc$ for some integer q.

Now $kd = k(au + bv) = (ka)u + (kb)v$

$= pcu + qcv$

$= (pu + qv)c$

Also $pu + qv$ is an integer : So, $c \mid kd$

Consequently, $kd = \gcd(ka, kb)$. So, $\gcd(ka, kb) = k \cdot \gcd(a, b)$.

Scanned with CamScanner

Definition Two integers a and b, not both zero, are said to be prime to each other (or relatively prime) if $\gcd(a,b) = 1$

Theorem 2.3.8. Let a and b be integers, not both zero. Then a and b are prime to each other if and only if $\exists$ integers u and v such that $1 = au + bv$

Proof: Let a and b be prime to each other. Then $\gcd(a, b) = 1$. So, $\exists$ integers u and v such that $1 = au + bv$.

Conversely, let us suppose that $\exists$ integers u and v such that $1 = au + bv$ and let $d = \gcd(a, b)$

Since $d|a$ and $d|b$ then $d|ax+by$ for all integers x and y.

Hence $d|au+bv = 1$ or $d|1$. This implies $d = 1$,

Since d is a positive integer. So, $\gcd(a, b) = 1$. So, a and b are prime to each other.

Theorem 2.3.9 If $d = \gcd(a, b)$, then $\frac{a}{d}$ and $\frac{b}{d}$ are integers prime to each other.

Proof: Since $d|a$, $\exists$ an integer m such that $md = a$

Since $d|b$, $\exists$ an integer n such that $nd = b$

As, $\frac{a}{d} = m$ and $\frac{b}{d} = n$, so, $\frac{a}{d}$ and $\frac{b}{d}$ are integers.

Since $d = \gcd(a,b)$, it is possible to find integers u and v such that $d = au + bv$

So, $1 = \left(\frac{a}{d}\right)u + \left(\frac{b}{d}\right)v$. This form of representation shows that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ by Theorem 2.3.8.

Hence $\frac{a}{d}$ and $\frac{b}{d}$ are prime to each other.

Theorem 2.3.10 If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

Proof: Since $\gcd(a,b) = 1$, $\exists$ integers u and v such that $1 = au + bv$. So, $c = acu + bcv$. Since $a \mid ac$ and $a \mid bc$ it follows that $a \mid (ac)u + (bc)v = c$. So, $a \mid c$

Corollary: If $ap = bq$ and a is prime to b then $a \mid q$ and $b \mid p$

Proof: As $a \mid bq$ and $\gcd(a,b) = 1$. So, $a \mid q$ by Theorem 2.3.10. Now $b \mid ap$ and $\gcd(a,b) = \gcd(b,a) = 1$. So, $b \mid p$ by Theorem 2.3.10

Theorem 2.3.11 If $a \mid c$ and $b \mid c$ with $\gcd(a,b) = 1$, then $ab \mid c$

Proof: Since $a \mid c$ and $b \mid c$, $\exists$ integers m and n such that $c = am = bn$. Since $\gcd(a,b) = 1$, $\exists$ integers u, v such that $1 = au + bv$. So, $c = (au)c + (bv)c = ab(un + vm)$

So, $ab \mid c$.