Note: Without the condition $\gcd(a,b)=1$, $a|c$, $b|c$ together may not imply $ab|c$

For example, $4|12$ and $6|12$ do not imply $4\times6|12$

Theorem 2.3.12 If a is prime to b and a is prime to c then a is prime to bc

Proof Since a is prime to b, $au+bv=1$ for some integers u,v. Since a is prime to c, $am+cn=1$ for some integers m,n

So, from $au+bv=1$,

$$acun+bcvn=cn=1-am \quad \text{as } am+cn=1$$

or, $$a(m+cun)+bc(vn)=1$$

Since $m+cun$ and vn are integers, it follows that a is prime to bc

---

Worked Examples (continued)

4. If a is prime to b, prove that $a+b$ is prime to ab

Solution: Since a is prime to b, $\exists$ integers u and v such that $au+bv=1$. This can be expressed as

$a(u-v)+(a+b)v=1$. Since $u-v$ and v are integers, it follows that a is prime to $a+b$.

Again $au+bv=1$ can be expressed as

$(a+b)u+b(v-u)=1$. Since $v-u$ and u are integers, it follows that $a+b$ is prime to b

By Theorem 2.3.12, $a+b$ is prime to ab

5. If a is prime to b, prove that

(i) a^2 is prime to b

(ii) a^2 is prime to b^2

Solution: Since a is prime to b, $\exists$ integers u and v such that $au + bv = 1$

Then $au = 1 - bv$

or, $a^2u^2 = 1 - 2bv + b^2v^2$

or, $a^2u^2 + b(2v - bv^2) = 1$

Since u^2 and $2v - bv^2$ are integers, it follows that a^2 is prime to b.

(ii) Since a^2 is prime to b, $\exists$ integers m and n such that $a^2m + bn = 1$. Then

$bn = 1 - a^2m$

or, $b^2n^2 = 1 - 2a^2m + a^4m^2$

or, $a^2(2m - a^2m^2) + b^2n^2 = 1$

Since n^2 and $(2m - a^2m^2)$ are integers, it follows that a^2 is prime to b^2

6. If $d = \gcd(a, b)$, show that $\gcd(a^2, b^2) = d^2$

Solution: Since $d = \gcd(a, b)$, $a = dp$ and $b = dq$ where p, q are integers prime to each other.

So, $a^2 = d^2p^2$, $b^2 = d^2q^2$ and this shows that

d^2 is a common divisor of a^2 and b^2

Let $\gcd(a^2, b^2) = d^2u$, where u is a positive integer.

Then $d^2u \mid d^2p^2$ and $d^2u \mid d^2q^2$ and so

$u \mid p^2$ and $u \mid q^2$.

But $\gcd(p, q) = 1 \Rightarrow \gcd(p^2, q^2) = 1$

Since u is a common divisor of p^2 and q^2

and $\gcd(p^2, q^2) = 1$, it follows that $u = 1$

Hence $\gcd(a^2, b^2) = d^2$

7. If $\gcd(a, b) = 1$ show that $\gcd(a+b, a^2-ab+b^2) = 1$ or 3

Solution: Let $d = \gcd(a+b, a^2 - ab+b^2)$. Then $d \mid a+b$

and $d \mid a^2-ab+b^2$. This implies

$d \mid (a+b)(a+b) - (a^2-ab+b^2)$, i.e., $d \mid 3ab$

So, $d \mid a+b$ and $d \mid 3ab$. Since $\gcd(a,b) = 1$, it follows that $\gcd(a+b, ab) = 1$. There exists integers u and v such that $u(a+b) + v(ab) = 1$. Since $d \mid a+b$

$(a+b) = dp$ for some integer p. So,

$upd + v(ab) = 1$. This show that d is prime to ab.

$d \mid 3ab$ and d is prime to ab implies $d \mid 3$. So,

$d = 1$ or $d = 3$

8. Prove that the product of any three

consecutive integers is divisible by 6.

Solution: By division algorithm, any integer, upon division by 3 leaves one of the remainders 0, 1, 2. So, any integer n is one of the form $3k$, $3k+1$, $3k+2$.

When $n = 3k$, n is divisible by 3

When $n = 3k+1$, $n+2$ is divisible by 3

When $n = 3k+2$, $n+1$ is divisible by 3

It follows that for any integer n, $n(n+1)(n+2)$ is divisible by 3

Again, the product of two consecutive integers is divisible by 2. So, $2 \mid n(n+1)(n+2)$ and $3 \mid n(n+1)(n+2)$. Since $\gcd(2,3) = 1$, it follows that $2 \times 3 = 6 \mid n(n+1)(n+2)$.

9. Prove that $1+2+\cdots+n$ is a divisor of $1^r + 2^r + \cdots + n^r$ for any odd positive integer r.

Solution: $1+2+\cdots+n = \frac{n(n+1)}{2}$. Let $S_n = 1^r + 2^r + \cdots + n^r$.

Then $2S_n = (1^r + n^r) + (2^r + (n-1)^r) + \cdots + (n^r + 1^r)$ ... (i)

Since r is an odd positive integer, $(n+1)$ is a divisor of each term in the right hand side of (i).

So, $(n+1) \mid 2S_n$ ... (ii)

Again $2S_n = [1^r + (n-1)^r] + [2^r + (n-2)^r] + \cdots + [(n-1)^r + 1^r] + 2n^r$ ... (iii)