Re: multiple.....

Source: http://sci.tech−archive.net/Archive/sci.math/2005−01/2494.html

---

mzafrullah_at_usa.net
Date: 01/09/05

```
Date: 8 Jan 2005 17:58:53 −0800
```

mina_world wrote:
> *hello......doctor~*
>
> *a,b,c,d,u is integers.*
>
> *if ac, bc+ad, bd is multiple of u,*
> *then bc, ad is multiple of u.*
> −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
> *i think.....*
>
> *bc+ac−ac−bd = (b−a)(c−d)*
> *so*
> *u|(b−a) or u|(c−d)*
>
> *if u|(b−a), then b−a = u.s, ac = u.t, bd = u.w*
> *i can deduce the fact that bc, ad is multiple of u.*
> *else if u|(c−d), similar.*
>
> *but*
> *if (b−a) and (c−d) is not multiple of u,*
> *(because, u is not prime)*
> *i can't deduce the result.*
>
> *so, i need your advice.*
>
> *thank you very much for your advice.*

Here's a somewhat simple solution.
Let r=GCD(a,b), so a=Ar, b=Br where A,B are coprime and so AX+B
is a primitive polynomial.
Next let s=GCD(c,d), so c=Cs, d=Ds and CX+D is a primitive polynomial
Note that (aX+b)(cX+d)=acX^2 +(bc+ad)X +bd ....(1)
Because u|ac,bc+ad,bd u divides the right hand side of (1) and hence
must divide the left hand side of (1). So
u|(aX+b)(cX+d)=rs(AX+B)(CX+D)
By Gauss' Lemma (AX+B)(CX+D) is primitive, being a product of primitive
polys
So any u in Z that divides rs(AX+B)(CX+D) must divide rs.

Now note r|a,b and s|c,d and this means that
rs|ac, ad, bc, bd−−>rs|bc,ad
But u|rs. So u|bc,ad.

It is interesting to note that "u|ac,bc+ad,bd−−>u|bc,ad" holds in an integrally
closed integral domain D (with qoutient field K) as well, as Bill Dubuque pointed out.
A simple way of seeing this is to note that (X−bc/u)(X−ad/u)=X^2 −((bc+ad)/u)X+abcd/(u^2)
is in D[X] (because u|ac,bd, u^2 |abcd and we are given that u|bc+ad). Now if D is integrally closed
and if f,g are monic polynomials in K[X] such that fg is in D[X] then both f and
g are in D[X].This follows from the following theorem which I stated and proved
in another post, but apparently some notation did not come out right.(Of course you would have to
chase some references.)
THEOREM Given an integral domain D with fraction field K,
the following are equivalent
(1) D is integrally closed (in its fraction field K)
(2) Every irreducible non−constant monic polynomial over D
is a prime in D[X].
(3) A, B in K[X], AB in D[X], (Ai)=1 for some i => B in D[x]
(4) A,B in K[X], AB in D[X] => Ai Bj in D
I would show the cycle: (1)−−>(4)−−>(3)−−>(2)−−>(1)
Proof. (4)<−−>(1) can be found as Theorem 1.5 of Mott, Nashier and Zafrullah, [
Contents of polynomials and invertibility, Comm. Algebra, 18(5) (1990) 1569−
1583]. (The language in this paper is that of contents of polynomials.) Here all we
need is (1)−−>(4) for this the proof of (1)−−>(6) on page 1573 of the Mott−Nashier−
Zafrullah paper appears to be the simplest. Next (4)−−>(3) is obvious. For (3)−−>(2)
proceed as follows.
Let f(X) be an irreducible monic polynomial in D[X] and suppose that f(X) is not a
prime in D[X] then f(X)=g(X)h(X) in K[X}. Because f is monic we can make both
g(X) and h(X) monics. But then by (3) both g(X) and h(X) are in D[x] a
contradiction. Hence every irreducible monic in D[X] is irreducible in K[X] and
hence a prime in D[X].
(2)−−>(1). Let u in K such that u satisfies a monic polynomial. Select a monic f(x) in
D of least degree such that f(u)=0. But then f(x) is irreducible in D[X] and hence a

prime in D[X] (by (2) which forces f(x) to be a prime, and hence irreducible in K[x]
. Yet as u is in K and f(u)=0 −−> f(x) has a linear factor in K[x] a contradiction
unless f(x) is linear, which forces u in D.
Note: Parts of this "Theorem" are quite well known. Here are some references:
(1)<−−>(2) appeared in Anderson and Zafrullah's, t−invertibility III [Comm. Algebra
21((1993), 1189−1209. It can also be deduced from S. McAdam's [Unique factorization of polynomials, Comm. Algebra 29(2001) 4341−4343.
(1)<−−>(3) is to be found in a paper to appear in Houston J. Math by Coykendall,
Dumitrescu and Zafrullah [The half−factorial property and domains of the form
A+XB[X].