Why do positive integers factor uniquely into primes? We learn this fact in elementary school, but is it really that trivial?   
  
For convenience we work with integers, rather than just positive integers. The integers [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)form a **ring** R, that is, addition and multiplication are defined so they are commutative, associative, and distributive; 0 is an additive identity and 1 is a multiplicative identity; additive inverses exist. An **integral domain** is a ring where no two nonzero elements multiply to 0.   
  
**1: [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)is an integral domain.**   
  
A **unit** of R has a multiplicative inverse in R. The units in [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)are 1 and -1.   
Say an element of R is **irreducible** if it is not a unit and it has no proper divisor.   
Say an element p is **prime** if p is not a unit, and [p|ab](http://www.artofproblemsolving.com/Forum/code.php?hash=04be2ebb9b3298c3fa54b4e4021132e6492611df&sid=25c8df611a228f61bf3e98fbcafe5afb)implies [p|a](http://www.artofproblemsolving.com/Forum/code.php?hash=7415ac7ab753300d4374ebcb12e7edff697b1c57&sid=25c8df611a228f61bf3e98fbcafe5afb)or [p|b](http://www.artofproblemsolving.com/Forum/code.php?hash=ea5727e9cbc3ad8b3864a1d5ac372ceb76273b87&sid=25c8df611a228f61bf3e98fbcafe5afb).   
It is not true in general that an irreducible element in a ring R is always a prime! Note that the definition of prime many people learn in elementary school is actually the definition for irreducible. In [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)these concepts are the same but we need to prove it.   
In [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)we can divide as follows: Given [a,b](http://www.artofproblemsolving.com/Forum/code.php?hash=5d8b1241b0484dd20c2cfeca6f692becfbab5d18&sid=25c8df611a228f61bf3e98fbcafe5afb)with [b\neq 0](http://www.artofproblemsolving.com/Forum/code.php?hash=821fbe5d0775069227086486dc14e497289bd979&sid=25c8df611a228f61bf3e98fbcafe5afb), we can write [a = qb + r](http://www.artofproblemsolving.com/Forum/code.php?hash=9ddea55a4fc1cb1e079034669c3975b5258d266f&sid=25c8df611a228f61bf3e98fbcafe5afb)where   
[0\leq r < |b|.](http://www.artofproblemsolving.com/Forum/code.php?hash=1efc1927940244e73e0c534de3eb67bc01044c0d&type=1&sid=25c8df611a228f61bf3e98fbcafe5afb)  
The last inequality is key: There exists a **norm** on [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)such that the remainder is "smaller" than the divisor; this norm is just the absolute value function. Thus we say that   
  
**2: [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)is an Euclidean domain.**   
  
An **ideal** I of a ring R is a subset such that if [a,b\in I](http://www.artofproblemsolving.com/Forum/code.php?hash=61e907e321bef4b6fa7941ee495e0413536fe0bf&sid=25c8df611a228f61bf3e98fbcafe5afb), then [ra,a + b\in I](http://www.artofproblemsolving.com/Forum/code.php?hash=c20fde2e0e10157e78fbe9259f858317cdc7f259&sid=25c8df611a228f61bf3e98fbcafe5afb)for any [r\in R](http://www.artofproblemsolving.com/Forum/code.php?hash=3217b37c71b163b0156bb8a40aa51c66046ed744&sid=25c8df611a228f61bf3e98fbcafe5afb). We can easily see that any set of the form [b\mathbb{Z} = \{bz|z\in \mathbb{Z}\}](http://www.artofproblemsolving.com/Forum/code.php?hash=cd3680fc01c56ff82b9461fa51135ba4161c8d7f&sid=25c8df611a228f61bf3e98fbcafe5afb)(the set of multiples of an integer [b](http://www.artofproblemsolving.com/Forum/code.php?hash=e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98&sid=25c8df611a228f61bf3e98fbcafe5afb)) is an ideal, but are these the only ones? We call these ideals **principal ideals**: they are generated by one element (here, [b](http://www.artofproblemsolving.com/Forum/code.php?hash=e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98&sid=25c8df611a228f61bf3e98fbcafe5afb)). A **principal ideal domain (PID)** is a ring where all ideals are principal.   
In [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb), suppose [I](http://www.artofproblemsolving.com/Forum/code.php?hash=ca73ab65568cd125c2d27a22bbd9e863c10b675d&sid=25c8df611a228f61bf3e98fbcafe5afb)is a nonzero ideal. Let [b](http://www.artofproblemsolving.com/Forum/code.php?hash=e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98&sid=25c8df611a228f61bf3e98fbcafe5afb)be the nonzero element of smallest absolute value.   
We can assume that [b](http://www.artofproblemsolving.com/Forum/code.php?hash=e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98&sid=25c8df611a228f61bf3e98fbcafe5afb)is positive since if [b\in I](http://www.artofproblemsolving.com/Forum/code.php?hash=beff059ebb50376acab168901db80ded7949e1fa&sid=25c8df611a228f61bf3e98fbcafe5afb)then [- b\in I](http://www.artofproblemsolving.com/Forum/code.php?hash=2d72fabb1beedcb35e15889da03bdc14fa4f1e71&sid=25c8df611a228f61bf3e98fbcafe5afb). Suppose [a\in I](http://www.artofproblemsolving.com/Forum/code.php?hash=b36dc5cdf3bcc0208bf87c0f98375fd5eabf0ed8&sid=25c8df611a228f61bf3e98fbcafe5afb). Then we can write [a = qb + r](http://www.artofproblemsolving.com/Forum/code.php?hash=9ddea55a4fc1cb1e079034669c3975b5258d266f&sid=25c8df611a228f61bf3e98fbcafe5afb)as above.   
We have [0\leq r < |b|](http://www.artofproblemsolving.com/Forum/code.php?hash=538ffa9fdf3142cac302885703fe6b3e1f349fda&sid=25c8df611a228f61bf3e98fbcafe5afb), but since [b](http://www.artofproblemsolving.com/Forum/code.php?hash=e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98&sid=25c8df611a228f61bf3e98fbcafe5afb)has minimal nonzero absolute value, [r = 0](http://www.artofproblemsolving.com/Forum/code.php?hash=25837e7083799548693252a0a9c374a149321947&sid=25c8df611a228f61bf3e98fbcafe5afb)and [b|a](http://www.artofproblemsolving.com/Forum/code.php?hash=2119dd3b0b4f7c488c19045b7bb9b8aaae184053&sid=25c8df611a228f61bf3e98fbcafe5afb). Thus [I](http://www.artofproblemsolving.com/Forum/code.php?hash=ca73ab65568cd125c2d27a22bbd9e863c10b675d&sid=25c8df611a228f61bf3e98fbcafe5afb)is principal. This idea can be abstracted to give:   
  
**3: An Euclidean domain is a principal ideal domain.**   
  
We say an integral domain is a **Unique Factorization Domain (UFD)** if every element (besides 0 and units) has a unique factorization into irreducible factors (up to units- in [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)this means up to a sign).   
Since every ideal in [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb)is principal, for every [a,b](http://www.artofproblemsolving.com/Forum/code.php?hash=5d8b1241b0484dd20c2cfeca6f692becfbab5d18&sid=25c8df611a228f61bf3e98fbcafe5afb)(not both 0) we have   
[a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=3bf22ae651e697950a59bdc1b892cde8297343d5&type=1&sid=25c8df611a228f61bf3e98fbcafe5afb)  
for some integer [d](http://www.artofproblemsolving.com/Forum/code.php?hash=3c363836cf4e16666669a25da280a1865c2d2874&sid=25c8df611a228f61bf3e98fbcafe5afb)(which can be assumed positive). This says there exists [p,q](http://www.artofproblemsolving.com/Forum/code.php?hash=d2926c1571d4e1b8561077d3308b7cfb6d211e59&sid=25c8df611a228f61bf3e98fbcafe5afb)such that   
[as + bt = d](http://www.artofproblemsolving.com/Forum/code.php?hash=5511fec9abec4bcebde6e3cca8caa89588019606&type=1&sid=25c8df611a228f61bf3e98fbcafe5afb)  
(Bezout's Theorem). From this, any divisor of [a,b](http://www.artofproblemsolving.com/Forum/code.php?hash=5d8b1241b0484dd20c2cfeca6f692becfbab5d18&sid=25c8df611a228f61bf3e98fbcafe5afb)must divide [d](http://www.artofproblemsolving.com/Forum/code.php?hash=3c363836cf4e16666669a25da280a1865c2d2874&sid=25c8df611a228f61bf3e98fbcafe5afb).   
[d](http://www.artofproblemsolving.com/Forum/code.php?hash=3c363836cf4e16666669a25da280a1865c2d2874&sid=25c8df611a228f61bf3e98fbcafe5afb)must divide [a,b](http://www.artofproblemsolving.com/Forum/code.php?hash=5d8b1241b0484dd20c2cfeca6f692becfbab5d18&sid=25c8df611a228f61bf3e98fbcafe5afb)since [a,b\in d\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=7cf00383986a0e84e4933d5732d49f09859f5835&sid=25c8df611a228f61bf3e98fbcafe5afb). Thus [d](http://www.artofproblemsolving.com/Forum/code.php?hash=3c363836cf4e16666669a25da280a1865c2d2874&sid=25c8df611a228f61bf3e98fbcafe5afb)is actually the **greatest common divisor** of [a,b](http://www.artofproblemsolving.com/Forum/code.php?hash=5d8b1241b0484dd20c2cfeca6f692becfbab5d18&sid=25c8df611a228f61bf3e98fbcafe5afb)!   
Now suppose [p](http://www.artofproblemsolving.com/Forum/code.php?hash=516b9783fca517eecbd1d064da2d165310b19759&sid=25c8df611a228f61bf3e98fbcafe5afb)is irreducible; we show [p](http://www.artofproblemsolving.com/Forum/code.php?hash=516b9783fca517eecbd1d064da2d165310b19759&sid=25c8df611a228f61bf3e98fbcafe5afb)is prime. Suppose [p|ab](http://www.artofproblemsolving.com/Forum/code.php?hash=04be2ebb9b3298c3fa54b4e4021132e6492611df&sid=25c8df611a228f61bf3e98fbcafe5afb)but [p](http://www.artofproblemsolving.com/Forum/code.php?hash=516b9783fca517eecbd1d064da2d165310b19759&sid=25c8df611a228f61bf3e98fbcafe5afb)does not divide [a](http://www.artofproblemsolving.com/Forum/code.php?hash=86f7e437faa5a7fce15d1ddcb9eaeaea377667b8&sid=25c8df611a228f61bf3e98fbcafe5afb). Then (the tricky part) using Bezout's Theorem and the fact that [\text{gcd}(p,a) = 1](http://www.artofproblemsolving.com/Forum/code.php?hash=7771b15c3d7f542c70dffd08ac238a67dd2d413e&sid=25c8df611a228f61bf3e98fbcafe5afb), we get [as + pt = 1](http://www.artofproblemsolving.com/Forum/code.php?hash=73ccc6f93cfa57894b71236ee601b3ca8e50d8a4&sid=25c8df611a228f61bf3e98fbcafe5afb)for some [s,t](http://www.artofproblemsolving.com/Forum/code.php?hash=ef28aeee727e0a8de667a5a258639ab3209c7ee5&sid=25c8df611a228f61bf3e98fbcafe5afb). Multiply by [b](http://www.artofproblemsolving.com/Forum/code.php?hash=e9d71f5ee7c92d6dc9e92ffdad17b8bd49418f98&sid=25c8df611a228f61bf3e98fbcafe5afb)to get   
[abs + ptb = b.](http://www.artofproblemsolving.com/Forum/code.php?hash=8414d2249f001fc1d57dcf70d7d7a996f5d24895&type=1&sid=25c8df611a228f61bf3e98fbcafe5afb)  
Since [p|ab|abs, p|ptb](http://www.artofproblemsolving.com/Forum/code.php?hash=27a5b6b02c4e80c0f275f8c3e13e73ad4ae5dddb&sid=25c8df611a228f61bf3e98fbcafe5afb), we have [p|b](http://www.artofproblemsolving.com/Forum/code.php?hash=ea5727e9cbc3ad8b3864a1d5ac372ceb76273b87&sid=25c8df611a228f61bf3e98fbcafe5afb). This shows that irreducible elements are prime in [\mathbb{Z}](http://www.artofproblemsolving.com/Forum/code.php?hash=b719c7ce5a7442a3bf64a8fa268fc460dcd2f3a3&sid=25c8df611a228f61bf3e98fbcafe5afb). (The reverse is also true.) Again, this argument can be abstracted to give:   
  
**4: In a PID, irreducible elements are prime.**   
  
Now in a PID, if an element factors into irreducible elements in two ways as   
[a_1\cdots a_m=b_1\cdots b_n](http://www.artofproblemsolving.com/Forum/code.php?hash=1ead5315b3e68697859dbbe637994bfea70cb0e5&type=1&sid=25c8df611a228f61bf3e98fbcafe5afb), we have [a_1](http://www.artofproblemsolving.com/Forum/code.php?hash=e86fe30994e484a6f59f315d1eeb57c2d8e80d78&sid=25c8df611a228f61bf3e98fbcafe5afb)dividing one of the [b_i](http://www.artofproblemsolving.com/Forum/code.php?hash=4790e84245a981b97634b391dde1fa0dffae8aab&sid=25c8df611a228f61bf3e98fbcafe5afb)since irreducible elements are prime. [b_i](http://www.artofproblemsolving.com/Forum/code.php?hash=4790e84245a981b97634b391dde1fa0dffae8aab&sid=25c8df611a228f61bf3e98fbcafe5afb)is irreducible so [a_1](http://www.artofproblemsolving.com/Forum/code.php?hash=e86fe30994e484a6f59f315d1eeb57c2d8e80d78&sid=25c8df611a228f61bf3e98fbcafe5afb)cannot be a proper divisor; [b_i/a_1](http://www.artofproblemsolving.com/Forum/code.php?hash=2116c7fd9e39a9c3f7aede110d6f84af64d0696d&sid=25c8df611a228f61bf3e98fbcafe5afb)is a unit. We divide out [a_1](http://www.artofproblemsolving.com/Forum/code.php?hash=e86fe30994e484a6f59f315d1eeb57c2d8e80d78&sid=25c8df611a228f61bf3e98fbcafe5afb)and repeat; all the factors on the left and right hand sides are matched, up to units (signs).   
  
**5: A principal ideal domain is a unique factorization domain.**   
  
**6: Unique factorization holds in [\mathbb{Z}.](http://www.artofproblemsolving.com/Forum/code.php?hash=137f5b91ba7d209686e458568a8b8bee0cc5c766&sid=25c8df611a228f61bf3e98fbcafe5afb)**