1. All you know is that $au + bv = 6$ for some integers a, b, u, v. What could (a, b) be? Also, is it possible that u and v are relatively prime?
2. Let $a, b \in \mathbb{Z}$. Suppose that a divides b and b divides a. Is it necessarily true that $a = b$? What can you say if $f(x)$ divides $g(x)$ and $g(x)$ divides $f(x)$ when $f(x), g(x) \in \mathbb{F}[x]$ for some field $\mathbb{F}$?
3. Let p be a positive prime integer. Show $\sqrt[3]{p}$ is irrational.
4. Does $2000x \equiv 4 \bmod 19875$ have any solutions? **No serious calculations needed!!!**
5. Write out a multiplication table for $\mathbb{Z}_3 \times \mathbb{Z}_2$. Find all units and zero divisors.
6. Let $U = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid a, b, c, d, e, f \in \mathbb{R} \right\}$ be the set of 3x3 real upper-triangular matrices. Show that U is a subring of $\mathbb{R}^{3\times 3}$.
7. Let R be a ring and define $Z(R) = \{r \in R \mid ar = ra \text{ for all } a \in R\}$ to be the *center* of R. Show that $Z(R)$ is a subring of R. What is $Z(\mathbb{Z})$? What is $Z(M(\mathbb{R}))$?
8. Show that $U(R_1 \times R_2) = U(R_1) \times U(R_2)$ for any two rings with identity R_1 and R_2.
9. Let R be a commutative ring with 1, and $r \in R$. Define $L_r : R \to R$ by $L_r(x) = rx$ for all $x \in R$. Prove that L_r is injective iff r is a nonzero nonzero divisor. Prove that L_r is sujective iff r is a unit.
10. Let $a, b \in R$ (a ring). Show that $-ab = (-a)b = a(-b)$ and $-(-a) = a$ just using ring axioms. Use your results above to show that $(-1)(-1) = 1$ if R has a multiplicative identity 1. One more thing...show that $3(ab) = (3a)b = a(3b)$.
11. Let R and S be rings. Prove that $R \times S$ is isomorphic to $S \times R$. Let R be an integral domain. Prove that $R \times R$ is *not* isomorphic to R.
12. Let $a, b, c \in \mathbb{Z}$. Show that if c divides b and $(a, b) = 1$, then $(a, c) = 1$. Now prove the same result for polynomials with field coefficients.
13. Is $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ a unit in $M(\mathbb{Z})$? Why or why not? Is A a unit in $M(\mathbb{Z}_7)$?
14. Factor $x^4 - 9$ in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$. Also, factor $x^4 - 9$ in $\mathbb{Z}_2[x]$.
15. Let $\mathbb{F}$ be a subfield of $\mathbb{C}$, $\phi : \mathbb{F} \to \mathbb{F}$ be an automorphism of $\mathbb{F}$ such that $\phi(c) = c$ for all $c \in \mathbb{Q}$ (ϕ fixes the rationals), and let $f(x) \in \mathbb{Q}[x]$. Show that $r \in \mathbb{F}$ is a root of $f(x)$ iff $\phi(r)$ is a root of $f(x)$.
16. Prove that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$. Also, prove that $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ defined by $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}[\sqrt{2}]$. In fact, using the previous problem, one can show that the only automorphisms of $\mathbb{Q}[\sqrt{2}]$ are ϕ and the identity map.
17. Let $f(x) \in \mathbb{F}[x]$ (where $\mathbb{F}$ is a field) be a polynomial of degree 5. Suppose that $f(x)$ has no roots in $\mathbb{F}$ and no quadratic factors (no polynomial of degree 2 divides $f(x)$). Can I then conclude that $f(x)$ is irreducible? Why or why not?