ELEMENTARY NUMBER THEORY

HOMEWORK 2

(1) Prove the following properties of gcd's:

(a) $\gcd(am, an) = a \gcd(m, n)$.

Let $d = \gcd(m, n)$. Then there are two things to show:

- $ad \mid am$, $ad \mid an$;
- $e \mid am$, $e \mid an$ implies $e \mid ad$.

From $d \mid m$, $d \mid n$ we get $ad \mid am$ and $ad \mid an$, and this shows that $ad \mid \gcd(am, an)$.
Now assume that $e \mid am$ and $e \mid an$. Bezout says $d = mx + ny$ for $x, y \in \mathbb{Z}$, hence $ad = amx + any$. Since e divides the terms on the right hand side, we conclude that $e \mid ad$.

You can also argue using unique factorization: write

$$m = \prod p_i^{m_i}, \quad n = \prod p_i^{n_i}, \quad a = \prod p_i^{a_i}.$$

Then the exponents in the prime factorization of d are $\min(m_i, n_i)$, as well as $a_i + \min(m_i, n_i)$ for ad and $\min(m_i + a_i, n_i + a_i)$ for $\gcd(am, an)$. Thus we need to show $\min(m_i + a_i, n_i + a_i) = a_i + \min(m_i, n_i)$, but this is clear.

(b) $\gcd(a, bc) \mid \gcd(a, b) \gcd(a, c)$.

Let $d = \gcd(a, bc)$, $e = \gcd(a, b)$ and $f = \gcd(a, c)$. We need to show $d \mid ef$ (Even if this is obvious, it is important to write it down since it will give you ideas how to proceed). Bezout gives $e = ar + bs$ and $f = at + cu$. Multiplying gives $ef = (ar + bs)(at + cu) = a(art + bst + cru) + bc(su)$. Since $d \mid a$ and $d \mid bc$, we conclude $d \mid ef$.

Again, here's the approach using unique factorization: write $a = \prod p_i^{a_i}$, $b = \prod p_i^{b_i}$, $c = \prod p_i^{c_i}$. Then $d = \gcd(a, bc) = \prod p_i^{\min(a_i, b_i + c_i)}$, and writing down similar formulas for $\gcd(a, b)$ and $\gcd(a, c)$ show that we have to prove $\min(a_i, b_i) + \min(a_i, c_i) \geq \min(a_i, b_i + c_i)$, which is easily seen to be true.

(c) If $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Write $d = am + bn$ (Bezout). Cancelling d gives $1 = \frac{a}{d}m + \frac{b}{d}n$. Thus any common divisor of m and n divides 1, and this implies the claim.

(d) If $ax + by = d$, then $\gcd(a, b) \mid d$; also show that it is not always true that $d = \gcd(a, b)$.

This is trivial: if $e = \gcd(a, b)$, then $e \mid a$, $e \mid b$, hence $e \mid (ax + by) = d$. Conversely, $2 = 1 \cdot 1 + 1 \cdot 1$ but $2 \neq \gcd(1, 1)$.

Remark: Consider the monoid $M = \{1, 4, 7, 10, \ldots\}$. Then $\gcd(4, 10) = 1$, but $\gcd(22 \cdot 4, 22 \cdot 10)$ does not exist: both 22 and 4 are common divisors, but none of them is greatest.

(2) Solve the diophantine equation $x^2 + 2y^2 = z^2$.

It is sufficient to look at primitive solutions, i.e. those with $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$. Then clearly x and z are odd. From $2y^2 = (z - x)(z + x)$ we see that $y = 2Y$ must be even; thus $2Y^2 = \frac{z-x}{2}\frac{z+x}{2}$.

Since the gcd of the factors on the right divides their sum z and their difference x, we conclude they must be coprime.

One of the factors on the right hand side must be even; replacing x by $-x$ if necessary we may assume that $\frac{z-x}{2}$ is even; then $Y^2 = \frac{z-x}{4}\frac{z+x}{2}$, and the factors are coprime. Thus $\frac{z-x}{4} = a^2$ and $\frac{z+x}{2} = b^2$. This implies $z = 2a^2 + b^2$ and $x = b^2 - 2a^2$, as well as $Y = ab$ and therefore $y = 2ab$. Thus the complete solution (under the assumption that $\frac{z+x}{2}$ is odd) is

$$x = b^2 - 2a^2, \quad y = 2ab, \quad z = b^2 + 2a^2.$$

(3) Prove, using the Euclidean algorithm, that $\gcd(am, an) = a \gcd(m, n)$.

Write $m - q_1 n = r_1$, $n - q_2 r_1 = r_2$ etc., where the r_i are determined uniquely by $0 \le r_1 < n$, $0 \le r_2 < r_1$ etc. The last nonzero remainder is then $\gcd(m, n)$.

Now multiply every line through by a. Then $0 \le ar_1 < an$, $0 \le ar_2 < ar_1$ etc., hence the new equations are what you would get by applying the Euclidean algorithm to am and an. Since the last nonzero remainder is $a \gcd(m, n)$, the claim follows.

(4) Using the last exercise, prove that if $a \mid mn$ and $\gcd(a, m) = 1$, then $a \mid n$. Hint: we have $\gcd(an, mn) = n$; now observe that a divides both an and mn.

$n = n \gcd(a, m) = \gcd(an, mn)$ and $a \mid mn$ imply $a \mid n$.

(5*) This problem was given to me by one of you. You may solve it if you want to: Show that 7 is the only prime $p \equiv 3 \bmod 4$ with the property that $p^2 - 3a^2 = 1$ for some a.

Hints: The equation $t^2 - mu^2 = 1$ is called the Pell equation. It has a nontrivial solution for every nonsquare $m > 0$. Let (x, y) denote the minimal solution in positive integers; then every solution (t, u) in positive integers comes from $t + u\sqrt{m} = (x + y\sqrt{m})^n$ for some $n \in \mathbb{N}$. In particular, the solutions of $p^2 - 3a^2 = 1$ come from $p_n + a_n\sqrt{3} = (2 + \sqrt{3})^n$.

(a) Show that $p_{n+1} > p_n$.

The minimal positive solution of the Pell equation $x^2 - 3y^2 = 1$ is $x = 2$, $y = 1$. We have $p_{n+1} + q_{n+1}\sqrt{3} = (p_n + q_n\sqrt{3})(2 + \sqrt{3}) = 2p_n + 3q_n + (2q_n + p_n)\sqrt{3}$, hence $p_{n+1} = 2p_n + 3q_n > p_n$.

(b) Show that p_n is even if and only if n is odd.

We have $(p1, q_1) = (2, 1)$ and $(p_2, q_2) = (7, 4)$. Now do induction. Assume n is odd and that p_n is even and q_n is odd; then $p_{n+1} = 2p_n + 3q_n$ is odd, and $q_{n+1} = 2q_n + p_n$ is even; similarly for even n.

(c) Show that p_n is divisible by 7 if $n \equiv 2 \bmod 4$.

Use induction. The claim is true for $n = 2$. Now observe $p_{n+4} + q_{n+4}\sqrt{3} = (p_n + q_n\sqrt{3})(2 + \sqrt{3})^4$. But $(2 + \sqrt{3})^4 = 97 + 28\sqrt{3}$, hence $p_{n+4} = 97p_n + 3 \cdot 28q_n$, and this is divisible by 7 because p_n and 28 are.

(d) Show that $p_n \equiv 1 \bmod 4$ if $4 \mid n$.

This is also clear by induction, since $p_{n+4} = 97p_n + 3 \cdot 28q_n \equiv p_n \bmod 4$.

Now the claim follows: If n is odd, then p_n is even; if $4 \mid n$, then $p_n \equiv 1 \bmod 4$; and if $n \equiv 2 \bmod 4$, then $7 \mid p_n$. Thus the only possible prime $p \equiv 3 \bmod 4$ of the form p_n is 7 itself, and this happens exactly for $n = 2$.