MATH 371
HOMEWORK SET 1
DUE 17.10.2012, WEDNESDAY

Remember: x, y, z, etc. a, b, etc. , A, B, etc. stand for integers! p stand ALWAYS for a prime number

(1) Show that

$$2^{32} + 1 \equiv 0(\bmod 641).$$

(Hint: Eliminate y from the equation $x^4 + y^4 = x^7 y + 1$ and use $2^4 + 5^4 = 2^7 5 + 1$)

Solution 1 (due to Coxeter?). *Note that* $5^4 + 2^4 = 5 \cdot 2^7 + 1 = 641$. *So* $641 | 2^{28}(2^4 + 5^4)$. *Since* $(x+1)|x^4 - 1$ *we also have* $641 | (5 \cdot 2^7)^4 - 1 = 5^4 \cdot 2^{28} - 1$. *So* 641 *divides the difference of two numbers:* $2^{28}(2^4 + 5^4) - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1$.

(2) Prove that if $2^k - 1$ is a prime number, then

$$2^{k-1}(2^k - 1)$$

is a perfect number.(Remember: A number n is called perfect if $\sigma(n) - n = n$.)

Solution 2. *Note the following:*

$$\begin{aligned}
\sigma(n) - n &= \sigma(2^{k-1}(2^k - 1)) - 2^{k-1}(2^k - 1) \\
&= \sigma(2^{k-1})\,\sigma(2^k - 1) - 2^{k-1}(2^k - 1), \ 2^k - 1 \textit{ is prime} \\
&= \frac{2^k - 1}{2 - 1}(1 + 2^k - 1) - 2^{k-1}(2^k - 1) \\
&= 2 \cdot 2^{k-1}(2^k - 1) - 2^{k-1}(2^k - 1) \\
&= n.
\end{aligned}$$

(3) Prove that if $f(n)$ is multiplicative then

$$g(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Solution 3. *Let* m *and* n *be two relatively prime integers. This implies that their set of divisors is disjoint. Hence we have:*

$$\begin{aligned}
g(m)\,g(n) &= \sum_{d|m} f(d) \sum_{e|n} f(e) \\
&= \sum_{d|m \textit{ and } e|n} f(d)d(e) \\
&= \sum_{d|m \textit{ and } e|n} f(d \cdot e) \\
&= \sum_{D|mn} f(D) \\
&= g(mn).
\end{aligned}$$

(4) Euler's totient or phi function, $\varphi(n)$ is a function that counts the number of positive integers less than or equal to n that are relatively prime to n. For example, $\varphi(6) = 1$ as there is only 5 which is both smaller than 6 and relatively prime to 6.

i. Compute $\varphi(p)$.

ii. Show that φ is multiplicative.(Recall that a function f is multiplicative if $f(m)f(n) = f(mn)$ whenever $(m, n) = 1$. Hint: You will need Chinese Remainder Theorem!)

iii. Find a formula for $\varphi(p^k)$.

Solution 4. i. *Since* p *is a prime, it is relatively prime to all numbers, except* 1*, smaller than* p*, that is* $\varphi(p) = p - 1$*, if* $p > 2$*.* $\varphi(3) = 1$*.*

ii. *Given two relatively prime integers* m *and* n *we have:*

$$\begin{aligned}\varphi(m)\,\varphi(n) &= \#\{d \mid d < m \text{ and } (d, m) = 1\} \cdot \#\{e \mid e < n \text{ and } (e, n) = 1\} \\ &= \#\{d \cdot e \mid d \cdot e < m \cdot n \text{ and } (d \cdot e, m \cdot n) = 1\} \\ &= \#\{D \mid D < m \cdot n \text{ and } (D, m \cdot n) = 1\} \text{ by Chinese Remainder Theorem} \\ &= \varphi(m \cdot n).\end{aligned}$$

iii.

$$\begin{aligned}\varphi(p^k) &= (\varphi(p))^k, \text{ by ii.} \\ &= (p-1)^k, \text{ by i.}\end{aligned}$$

if p *is an odd prime.* $\varphi(2^k) = \#\{$ *odd numbers satisfying* $1 < d < 2^k\}$ *for any* k*.*

(5) Find x and y satisfying

$$54x + 17y = 136$$

Solution 5. *Note that* 54 *and* 17 *are relatively prime with*

$$6 \cdot 54 + (-19)17 = 1$$

. So, $x = 136 \cdot 6$ *and* $y = 136 \cdot (-19)$ *are solutions of the above Diophantine equation.*

(6) If exists, find all solutions of

$$39x + 47y = 4151$$

in positive integers.

Solution 6. *Note again* $(-6)39 + 5\,47 = 1$*. By Theorem 4 in our notes, we know that all solutions are of the form:*

$$x = -6 + t \cdot 47 \text{ and } y = 5 + t \cdot 39$$

As we want all the solutions to be in positive integers $x = -6 + t \cdot 47$ *implies that* $t \geq 1$*. And for every such* t *both components are positive. Thus, all positive solutions are:*

$$\{(x, y) \mid x = -6 + t \cdot 47 \text{ and } y = 5 + t \cdot 39,\ t > 0\}.$$

Note: For your future Euclidean algorithm computations you may use the web-site `http://www.math.sc.edu/~sumner/numbertheory/euclidean/euclidean.html`

(7) Show that if there are integer solutions to the equation

$$ax + by + cz = d$$

then the greatest common divisor of a, b and c divides d

Solution 7. *Let* x_o*,* y_o *and* z_o *be the integer solutions, and let* D *be the greatest common divisor of* a*,* b *and* c *and write* $a = D\,a'$*,* $b = D\,b'$ *and* $c = D\,c'$*. Then*

$$d = ax + by + cz = D(a'x + b'y + c'z).$$

Thus $D|d$*.*

(8) Prove Theorem 5 in your notes.

Solution 8. *See* `http://fermatslasttheorem.blogspot.com/2005/05/pythagorean-triples-solution.html` *for a readable proof.*

(9) If x_o, y_o, z_o are integers satisfying

$$x^2 + y^2 + z^2 = 3xyz$$

then show that $x_1 = x_o$, $y_1 = y_o$ and $z_1 = 3x_oy_o - z_o$ are also solutions. Describe in detail how this can be used to find infinitely many solutions in positive integers starting with $x_o = y_o = z_o = 1$.

Solution 9. *Let us first show that* $x_1 = x_o$, $y_1 = y_o$ *and* $z_1 = 3x_oy_o - z_o$ *are solutions. For this:*

$$\begin{aligned} x_1^2 + y_1^2 + z_1^2 &= x_o^2 + y_o^2 + (3x_oy_o - z_o)^2 \\ &= x_o^2 + y_o^2 + 9x_o^2\, y_o^2 - 6x_o\, y_o\, z_o + z_o^2 \\ &= 3x_oy_oz_o + 9x_o^2\, y_o^2 - 6x_o\, y_o\, z_o \\ &= 9x_o^2\, y_o^2 - 3x_o\, y_o\, z_o \\ &= 3x_oy_o(3x_oy_o - z_0) \\ &= 3x_1y_1z_1. \end{aligned}$$

Note also that $x_o = y_o = z_o = 1$ *is a solution. However, a direct use of this this solution will not give rise to infinitely many solutions. But, replacing* z_i *by* y_i *and using the above formulae we get:*

$$\begin{aligned} x_o = y_o = z_o = 1 \quad &\longrightarrow \quad x_1' = 1, y_1' = 1, z_1' = 3x_oy_o - z_o = 3 - 1 = 2 \longrightarrow x_1 = 1, y_1 = 2, z_1 = 1 \\ &\longrightarrow \quad x_2' = 1, y_2' = 2z_2' = 3x_1y_1 - z_1 = 6 - 1 = 5 \longrightarrow x_2 = 1, y_2 = 5, z_2 = 2 \\ &\longrightarrow \quad x_3' = 1, y_3' = 5z_3' = 3x_2y_2 - z_2 = 15 - 2 = 13 \longrightarrow x_3 = 1, y_3 = 13, z_3 = 5 \\ &\longrightarrow \quad ... \end{aligned}$$

(10) i. Given a binary quadratic form $f(x, y) = Ax^2 + Bxy + Cy^2$ with Δ is a perfect square describe all solutions of the equation

$$f(x, y) = p.$$

assuming $(A, B, C) = 1$.

ii. Explain what happens if $(A, B, C) \neq 1$.

iii. Use your previous result to find all solutions of the equation

$$2x^2 + 5xy + 2y^2 = 5$$

Solution 10. i. *If* Δ *is a perfect square then* $f(x, y)$ *can be written as a product of two linear factors having integer coefficients:*

$$(\alpha\, x + \beta\, y)(\gamma\, x + \delta\, y).$$

Since we are interested in integer solutions, it is enough to solve the following two system of linear Diophantine equations:

$$\alpha\, x + \beta\, y = \pm 1 \textit{ and } \gamma\, x + \delta\, y = \pm p$$
$$\alpha\, x + \beta\, y = \pm p \textit{ and } \gamma\, x + \delta\, y = \pm 1.$$

The two systems are symmetric, so we'll focus on the first one. In order $\gamma\, x + \delta\, y = \pm p$ *to have solution* $(\gamma, \delta) = 1$ *or* p*. However if* $(\gamma, \delta) = p$ *we have* $p|A = \alpha\, \gamma$, $p|B = \alpha\, \delta + \beta\, \gamma$ *and* $p|C = \beta\, \delta$*, but we assumed that the greatest common divisor of* A, B *and* C *is* 1*, contradiction. So, we must have both* $(\alpha, \beta) = 1$ *and* $(\gamma, \delta) = 1$*. Otherwise there are no solutions. The solution set is then the common solutions of the first system union the solutions of the second system.*

ii. *If the greatest common divisor of* A, B *and* C *is not* 1*, or* p *then the equation does not have any solution!*

iii. *The greatest common divisor of* 2 *and* 5 *is* 1*. And* $\Delta = B^2 - 4AC = 9 = 3^2$ *so we will solve*

$$2x^2 + 5xy + 2y^2 = (2x + y)(x + 2y) = 5$$

We have to solve four equation systems. The first one is

$$2x + y = 1 \textit{ and } x + 2y = 5.$$

A solution to the first one is $x = 1$, $y = -1$*, so all solutions can be written as* $x = 1 + t\,1$ *and* $y = -1 - t\,2$*. All solutions to the equation*

$$x + 2y = 5$$

are given as $x = 1 + 2\,s$ *and* $y = 2 - s$*. We must have*

$$\begin{aligned} 1 + t = 1 + 2\,s \textit{ and } -1 - 2t = 2 - s \quad &\Leftrightarrow \quad t = 2s \textit{ and } s - 2t = 3 \\ &\Leftrightarrow \quad s = -1 \textit{ and } t = -2. \end{aligned}$$

All the remaining cases:

$$2x + y = -1 \textit{ and } x + 2y = -5$$
$$2x + y = 5 \textit{ and } x + 2y = 1$$
$$2x + y = -5 \textit{ and } x + 2y = -1$$

are solved in a similar fashion.