Homework 3 Due 18:00, October 27, 2021

Cristian Brinza FAF 212

Problem 4.1

Read the amazing story on the proof of Fermat Theorem from Simon Singh blog post "The whole Story". The link is provided on the course web page on ELSE platform.

Problem 4.2

Prove the following properties for any integers *a, b*:

a) $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.

$$\gcd(ka, kb) = s \cdot ka + t \cdot kb = k(sa + tb) = k \cdot \gcd(a, b) \; for \; all \; k > 0$$

b) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

$$\exists s, t \rightarrow sa + tb = 1 \, , \exists s_1, t_1 \rightarrow s_1 a + t_1 b = 1 :$$

$$1) \; sa + tb = 1 \cdot (t_1, c) \rightarrow st_1 ca + tt_1 cb = 1 \rightarrow \; s_1 a + t_1 cta + t_1 \text{ctb} = t_1 c + s_1 a \rightarrow$$

$$(s_1 + st_1 c)a + (tt_1)cb = 1 \rightarrow \; gcd(a, bc) \; = \; 1.$$

c) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

$$if \; gcd(a, b) = 1 \rightarrow sa = tb = 1 \rightarrow \cdot \; c = cas + ctb = c, (we \; can \; write \text{ "a·n" as "b · c" , so}$$
$$because \; a|bc \rightarrow \text{csa+tan=c, as a(cs+tn)=c ,then (cs+tn) we can substitute as x - so } a|c$$

Problem 4.3

A number is called **perfect** if it is equal to the sum of its positive divisors, other than itself. For example, 6 = 1 + 2 + 3 or 28 = 1 + 2 + 4 + 7 + 14 are perfect numbers.

Explain why $2^{k-1}(2^k - 1)$ is perfect, when $2^k - 1$ is a prime number.

$$We \; have \; 2^k - 1 - prime, then \; 2^{k-1}(2^k - 1) \; have \; the \; devisors : 1,2,4, \dots, 2^{k-1}, which \; sum \; to \; 2^k - 1 \rightarrow$$
$$1 \cdot (2^k - 1), 2 \cdot (2^k - 1), 4 \cdot (2^k - 1), \dots, 2^{k-2}(2^k - 1), which \; sum \; to \; (2^{k-1} - 1)(2^k - 1), so$$
$$\rightarrow \; 2^{k-1}(2^k - 1) - perfect \; sum$$

Problem 4.4

Use the Extended Euclid Algorithm (Pulverizer) to find the greatest common divisors and integers *st* and *t* such that

a) $\gcd(60, 21) = s \cdot 60 + t \cdot 21$;

$$gc\,d(60,21) = gcd(21,18) \rightarrow 60 = 2 \cdot 21 + 18, sogc\,d(18,3) = gc\,d(3,0) \rightarrow 10 = a - 2b, as$$
$$3 = b - 18 = b - (a - 2b) = b - a + 2b = \; -a + 3b;$$
$$\text{Therefor s} = -1, \text{t} = 3 \rightarrow gc\,d(60,21) = -1 \cdot 60 + 3 \cdot 21$$

b) $\gcd(42, 360) = s \cdot 42 + t \cdot 360$.

$$gcd(42,24) \; as \; 24 = b - 8a \; ; \qquad \gcd(24,18) \; as \; 18 = a - 24 = a - b + 8a;$$
$$\gcd(18,6) \; as \; 6 = 24 - 18 = b - 8a - a + b - 8a, \quad so \; \gcd(6,0) \; as = 2b - 17a \rightarrow s = \; -17, t = 2;$$
$$so \; \gcd(42,360) = \; -17 \cdot 42 + 2 \cdot 360$$

Problem 4.5

Let $m = 2^9 5^{24} 11^7 17^{12}$ and $n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2$.

What is the gcd(*m, n*)?

$$m = 2^9 5^{24} 11^7 17^{12}, as\ n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2, so\ gnd(m,n) = 2^3 11^7 17^9$$

.

Problem 4.6

Let $n = 11$ and consider modular classes modulo 11 (denoted by [*x*]). Compute:

a) $[4] + [8] = [12] = [1]_{11}$;

b) $[3] - [9] = [5]$;

c) $[6] \cdot [5] = [30] = [8]_{11}$;

d) $[8]^{-1} = (8 \cdot u = [1], u = 7 \rightarrow 8 \cdot 7 = [1]_{11}) = [7]$;

e) $[7] \cdot [6]^{-1} = [7 \cdot 2] = [3]$.

f) $[5] - [10]^{-1} = [-5] = 6$.

Problem 4.7

Repeat previous problem with $n = 12$. Compute:

b) $[4] + [8] = 0$;

b) $[3] - [9] = 6$;

c) $[6] \cdot [5] = 6$;

d) $[8]^{-1} = (There\ is\ no\ modular\ multiplicative\ inverse\ for\ this\ integer)$;

e) $[7] \cdot [6]^{-1} = (There\ is\ no\ modular\ multiplicative\ inverse\ for\ this\ integer)$;.

f) $[5] - [10]^{-1} = (There\ is\ no\ modular\ multiplicative\ inverse\ for\ this\ integer)$.

Problem 4.8

a) Use the Extended Euclid Algorithm (Pulverizer) to find the multiplicative inverse of 19 modulo 31 in therange {0,…,30}.

$$19x \equiv z\ (mod 31)$$
$$19^2 = 361 \equiv 20 (\text{mod } 31)$$
$$19^3 = 6859 \equiv 8 (\text{mod } 31)$$
$$19^6 = (19^3)^2 \equiv 8^2 \equiv 2 (\text{mod } 31)$$
$$19^{12} = (19^6)^2 \equiv 2^2 \equiv 4 (\text{mod } 31)$$
$$then \rightarrow\ 19^{29} = (19^{12})^2 * 19^3 *\ 19^2 =\ 4^2 * 8 * 20 = 2560 = 18 (\text{mod } 31) \rightarrow$$
$$thus\ 19 * 18 = 342 \equiv 1 (\text{mod } 31) \rightarrow 11 \cdot 31 + 1.$$

b) Use Little Fermat Theorem to find the multiplicative inverse of 19 modulo 31 in the range {0,…,30}.

$$a^{p-1} \equiv 1\ (mod\ p) \rightarrow\ 19^{p-1} =\ 1\ (mod\ 31) \rightarrow$$
$$19^{p-1} = \equiv 1 (\text{mod } p) \rightarrow$$
$$19^{31-1} = 1\ (mod\ 31) \rightarrow$$
$$19^{30} = 1\ (mod\ 31) \rightarrow$$
$$19^{30} = 1\ (mod\ 31) \rightarrow\ 30$$

c) Compute 19^{147} modulo 17.

Problem 4.9

Let $\phi(n)$ be the totient function (Euler function). Find

a) $\phi(18) = card\{1,5,7,11,13,17\} = 6 \; or = \phi(2 \cdot 3^2) = 18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = \frac{36}{6} = 6$;

b) $\phi(170) = \phi(2 \cdot 5 \cdot 17) = 170\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{17}\right) = 64$;

c) $\phi(400)\ ) = \phi 2^4 \cdot 5^2 = 400\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400 \cdot \frac{1}{2} \cdot \frac{4}{5} = 160$.