Modular Arithmetic

September 26, 2009

***Theorem 1*: For all $k \in \mathbb{Z}^+$, $\gcd(mk, nk) = k\gcd(m, n)$.**

Proof: By definition of greatest common divisor, we can say that $\gcd(mk, nk) = amk + bnk$ for some $a, b \in \mathbb{Z}$. By factoring, we obtain $k(am + bn)$. Again, by defintion of greatest common divisor, we obtatin $k\gcd(m, n)$. ■

***Theorem 2*: For all positive integers a, b, and s, if $\gcd(s, a) = 1$ and $\gcd(s, b) = 1$, then $\gcd(s, ab) = 1$.**

Proof: Since $\gcd(s, a) = 1$, we can say that $ms + na = 1$ for some $m, n \in \mathbb{Z}^+$. Likewise, since $\gcd(s, b) = 1$, we can say that $ps + qb = 1$ for some $p, q \in \mathbb{Z}^+$. By multiplication, we have that $(ms + na)(ps + qb) = 1$. By expansion, we have that $msps + msqb + naps + naqb = 1$. By factoring, we have that $s(mps + mqb + nap) + ab(nq) = 1$. By closure of integers, we obatin $s(v) + ab(w) = 1$ for some $v, w \in \mathbb{Z}$. Hence, $\gcd(s, ab) = 1$. ■

***Theorem 3*: Let a, b, and p be integers such that p is a prime. If $p|ab$, then $p|a$ or $p|b$.**

Proof:

Suppose that $p|ab$, but p does not divide a. This would imply that $\gcd(p, a) = 1$. Thus, we have that $cp + ad = 1$ for some integers $c, d \in \mathbb{Z}$. By multiplying by b, we see that $b(cp + ad) = b \Leftrightarrow bcp + bad = b$. Since $p|ab$, we can rewrite $bcp + bad = b$ as $bcp + pkd = b$ for some $k \in \mathbb{Z}$. By factoring, we have that $p(bc + kd) = b$. Hence, $p|b$. Similarly, suppose that $p|ab$, but p does not divide b. This would imply that $\gcd(p, b) = 1$. Thus, we have that $cp + bd = 1$ for some integers $c, d \in \mathbb{Z}$. By multiplying by a, we see that $a(cp + bd) = a \Leftrightarrow acp + abd = a$. Since $p|ab$, we can rewrite $acp + abd = a$ as $acp + pkd = a$ for some $k \in \mathbb{Z}$. By factoring, we have that $p(ac + kd) = a$. Hence, $p|a$. ■

***Theorem 4*: If a, b, and c are integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.**

Proof: By definition of greatest common divisor, since $\gcd(a, b) = 1$, we have that $ax + by = 1$ for some $x, y \in \mathbb{Z}$. If we multiply by c, then we obtain $c(ax + by) = c \Leftrightarrow cax + cby = c$. Since $a|bc$, we can rewrite $cax + cby = c$ as $cax + aky = c$ for some $k \in \mathbb{Z}$. By factoring, we obtain $a(cx + ky) = c$. By definition of divisibility, we see that $a|c$. ■

***Theorem 5*: Let p be a prime. Then $(a + b)^p \equiv a^p + b^p \pmod{p}$.**

Proof: By the Binomial Theorem, $(a + b)^p = \binom{p}{0}a^pb^0 + \binom{p}{1}a^{p-1}b^1 + ... + \binom{p}{p-1}a^1b^{p-1} + \binom{p}{p}a^0b^p = a^p + pa^{p-1}b + ... + pab^{p-1} + b^p = p(a^{p-1}b + ... + ab^{p-1}) + a^p + b^p$. Now, all terms except for the a^p and b^p terms are all divisible by p. This implies that $(a + b)^p - (a^p + b^p) = kp$ for some integer k. By definition of congruence modulo, we can say that $(a + b)^p \equiv a^p + b^p \pmod{p}$ as desired. ■

Let $n \in \mathbb{Z}^+ \setminus \{1\}$. Define $g : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $g([r]_n, [s]_n) = [r+s]_n$. Prove that g is a well-defined function.

Proof: If $[r_1]_n = [r_2]_n$ and $[s_1]_n = [s_2]_n$, then $r_1 \equiv r_2 \pmod{n}$ and $s_1 \equiv s_2 \pmod{n}$. By definition of congruence modulo, we have that $r_1 - r_2 = jn$ for some $j \in \mathbb{Z}$ and $s_1 - s_2 = kn$ for some $k \in \mathbb{Z}$. By addition, we have that $(r_1 - r_2) + (s_1 - s_2) = jn + kn = n(j+k) = r_1 + s_1 - (r_2 + s_2)$. This implies that $r_1 + s_1 \equiv r_2 + s_2 \pmod{n}$, and hence, we have that $[r_1 + s_1]_n = [r_2 + s_2]_n$. Thus, g is well-defined. ■

Prove that the function $\phi(2n) = \begin{cases} \phi(n) & \text{if } n \in 2\mathbb{Z}+1 \\ 2\phi(n) & \text{if } n \in 2\mathbb{Z} \end{cases}$ is well-defined.

Proof: If $n \in 2\mathbb{Z}+1$, then $\gcd(2, n) = 1$, so we have that $\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n)$. Now, if $n \in 2\mathbb{Z}$, then $n = 2^k m$ for some integer k and some odd integer m. By substitution and multiplicative identities, we have that $\phi(2n) = \phi(2 \cdot 2^k m) = \phi(2^{k+1}m) = \phi(2^{k+1})\phi(m)$. By Euler's identity, we have that $\phi(2^{k+1})\phi(m) = [2^{k+1}(1 - \frac{1}{2})]\phi(m) = [2^{k+1}(\frac{1}{2})]\phi(m) = 2^k\phi(m) = 2(2^{k-1})\phi(m)$. By reversing Euler's identity, we have that $2(2^{k-1})\phi(m) = 2\phi(2^k)\phi(m) = 2\phi(2^k m)$. Finally, by back-substitution, we obtain $2\phi(n)$ as desired. Hence, the function is well-defined. ■

Let $x \in \mathbb{Z}$. Define $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ by $f([x]_{12}) = [3x]_{24}$. Explain why f is not a well-defined function.

Suppose we have two integers, m and n, with $m = 0$ and $n = 12$. Since $[0]_{12} = 0$ and $[12]_{12} = 0$, then clearly $m = n$. However, $f([3(0)]_{24}) = [0]_{24} = 0$, whereas $f([3(12)]_{24}) = [36]_{24} = 12$, so $f(m) \neq f(n)$.