Notebook Swag

Sam Grayson

April 22, 2015

4.1 Exercise: Write out the powers of 2 mod 7

$$\begin{aligned} 2^0 \pmod 7 &\equiv 1 \\ 2^1 \pmod 7 &\equiv 2 \\ 2^2 \pmod 7 &\equiv 4 \\ 2^3 \pmod 7 &\equiv 1 \\ 2^4 \pmod 7 &\equiv 2 \\ 2^5 \pmod 7 &\equiv 4 \\ 2^6 \pmod 7 &\equiv 1 \end{aligned}$$

4.2 Theorem: Coprime numbers raised to any power are still coprime.

Let $a, n \in \mathbb{Z}$ where $\gcd(a, n) = 1$. This proof applies for all $j \in \mathbb{N}$. Show $\gcd(a^j, n) = 1$

Proof: I will begin by using the tools developd in chapter 2, $\mathrm{pf}(a) \cap \mathrm{pf}(n) = \{\}$. $\min(x\#\,\mathrm{pf}(a), x\#\,\mathrm{pf}(b)) = 0$. Since $\min(a, b) = a \vee \min(a, b) = b$, $0 = \mathrm{pf}(a) \vee 0 = \mathrm{pf}(b)$. If $0 = \mathrm{pf}(a)$, then $x\#\,\mathrm{pf}(a) = 0$, furthermore no matter how many a's $x\#\,\mathrm{pf}(a^j) = 0$ (since $x\#\,\mathrm{pf}(a) = 0 = j(x\#\,\mathrm{pf}(a)) = x\#\,\mathrm{pf}(a^j)$). Thus $\min(x\#\,\mathrm{pf}(a^j), x\#\,\mathrm{pf}(b)) = 0$. Otherwise $0 = \mathrm{pf}(b)$, then no matter what $x\#\,\mathrm{pf}(a^j)$ is, $\min(x\#\,\mathrm{pf}(a^j), x\#\,\mathrm{pf}(b)) = 0$. Thus $\gcd(a^j, n) = 1$. This conditional proof shows $\gcd(a, n) = 1 \rightarrow \gcd(a^j, n) = 1$. ∎

This proof can also be written using 1.43.

4.3 Theorem: If b is congruent to a coprime of n mod n, then b is a coprime of n.

Let $b \equiv a \pmod n$ and $\gcd(a, n) = 1$. Show $\gcd(a, b) = 1$

Proof: Assume for contradiction $b = nc$ for some c. Then $b \equiv a \pmod n$ means $n|(nc - a)$. This is problematic because then $nj = nc - a$, and then $n(c - j) = a$. Therefore $b \neq nc$. Therefore by definition of greatest common divisor $\gcd(b, n) = 1$. In conclusion $(\gcd(a, n) = 1 \wedge b \equiv a \pmod n) \rightarrow \gcd(a, b) = 1$. ∎

4.4 Theorem: All numbers have at least two different exponents that give the same result.

Let $a, n \in \mathbb{N}$. Assume $\neg\exists a^i \not\equiv a^j \pmod n$ for contradiction.

Proof: For $i \in \{1, 2, \ldots, n\}$, $\neg\exists a^i \not\equiv a^j \pmod n$. These n noncongruent integers form a CRS by Theorem 3.17. a^{n+1} must be congruent to something in the CRS by the definition of CRS. Therefore $\exists j(a^{n+1} \equiv a^j \pmod n)$. This can not be the case since it denies the contradictive assumption. Therefore $\exists i, j \in \mathbb{N}(i \neq j \wedge a^i \equiv a^j \pmod n)$. ∎

4.5 Theorem: The converse of Theorem 1.14 is true if $\gcd(c, n) = 1$.

Let $a, b, c, n \in \mathbb{N}$. Let $ac \equiv bc \pmod{n}$. Show $a \equiv b \pmod{n}$

Proof: The first congruence translates to $n|(ac - bc)$ or $n|c(a - b)$. By Theorem 1.41, $n|(a-b)$ (since $\gcd(a, n) = 1$, no factor of c can be divided by n). Therefore $a \equiv b \pmod{n}$. In conclusion $ac \equiv bc \wedge \gcd(c, n) = 1 \rightarrow a \equiv b$. ■

4.6 Theorem: If a number is coprime to the modulo, it has at least one power congruent to one.

Let $\gcd(a, n) = 1$. Show $\exists k \in \mathbb{N}(a^k \equiv 1 \pmod{n}$

Proof: $a^i \equiv a^j \pmod{n}$ WLOG $i \geq j$ by 4.4. $\frac{a^i}{a^j} \equiv {}^{a}\gcd(a, n) = 1 \rightarrow \exists k \in \mathbb{N}(a^k \equiv 1 \pmod{n}))$. ■