# Notebook Swag

Sam Grayson

April 29, 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 developed in Chapter 2, $\text{pf}(a) \cap \text{pf}(n) = \{\}$. $\min(x\#\,\text{pf}(a), x\#\,\text{pf}(b)) = 0$. Since $\min(a, b) = a \vee \min(a, b) = b$, $0 = \text{pf}(a) \vee 0 = \text{pf}(b)$. If $0 = \text{pf}(a)$, then $x\#\,\text{pf}(a) = 0$, furthermore no matter how many a's $x\#\,\text{pf}(a^j) = 0$ (since $x\#\,\text{pf}(a) = 0 = j(x\#\,\text{pf}(a)) = x\#\,\text{pf}(a^j)$). Thus $\min(x\#\,\text{pf}(a^j), x\#\,\text{pf}(b)) = 0$. Otherwise $0 = \text{pf}(b)$, then no matter what $x\#\,\text{pf}(a^j)$ is, $\min(x\#\,\text{pf}(a^j), x\#\,\text{pf}(b)) = 0$. Thus $\gcd(a^j, n) = 1$. This conditional proof shows $\gcd(a, n) = 1 \to \gcd(a^j, n) = 1$. ∎

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 $(\gcd(a, n) = 1 \wedge b \equiv a \pmod n) \to \gcd(a, b) = 1$. ∎

**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 Theorem 4.4. $\frac{a^i}{a^j} \equiv \frac{a^j}{a^j} \pmod{n}$ by Theorem 4.5, or equivalently $a^{i-j} \equiv a^{i-i} \equiv 1 \pmod{n}$. Therefore when $k = i - j$, $a^k \equiv 1 \pmod{n}$. In conclusion $\gcd(a, n) = 1 \rightarrow \exists k \in \mathbb{N}(a^k \equiv 1 \pmod{n})$. ∎

**4.13 Theorem:** Let $S = \{a, 2a, 3a, \ldots, pa\}$ where $\gcd(a, p) = 1$. $S$ is a complete residue system modulo $p$.

**Proof:** Let $R = \{1, 2, 3, \ldots, p\}$. $R$ is the canonical complete residue system modulo $p$. Therefore all elements of $R$ are pairwise incongruent $\forall i, j(i \neq j \rightarrow i \not\equiv j \pmod{p})$. The contrapositive of theorem 4.5 states that $i \not\equiv j \pmod{n}$ implies $ai \not\equiv aj \pmod{n}$. Therefore the elements of $R$ are also pairwise incongruent. By Theorem 3.17, any set of $p$ pairwise incongruent integers form a complete residue system modulo $p$.

**4.14 Theorem:** Let $p \in \mathbb{P}$ and $a \nmid p$. $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$.

Let $R = \{a, 2a, 3a, \ldots, (p-1)a, pa\}$ and $S = \{1, 2, 3, \ldots, p-1, p\}$.

**Proof:** $R$ consitutes a complete residue system by Theorem 3.14. $S$ is the canonical complete residue system. Therefore every element of $R$ is congruent to exactly one thing in $S$ and everything in $S$ is congruent to exactly one thing in $R$. Therefore there is a one-to-one mapping of congruent elements from $S$ to $R$. $p|pa \wedge p|p$, therefore $pa \equiv 0 \equiv p \pmod{p}$. Therefore there is a one-to-one mappnig of congruent elements from $R \setminus \{pa\}$ to $S \setminus \{p\}$. For each element pair $r_i$ and $s_i$ in $R \setminus \{pa\}$ and $S \setminus \{p\}$, we can multiply the left-hand side of the equation $1 \equiv 1 \pmod{p}$ by $r_i$ and the right-hand side by $s_i$. In the end, we will get all of the elements of $R \setminus \{pa\}$ multiplied together are equivalent to all of the elements of $S \setminus \{p\}$. $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$. ∎

**4.15 Theorem:** In a prime modulo, an integer not divisible by the modulo raised to the $(p-1)$-th power is congruent to one.

Let $p \in \mathbb{P}$ and $a \in \mathbb{Z} \wedge p \nmid a$. $a^{p-1} \equiv 1 \pmod{p}$.

**Proof:** $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{n}$ by Theorem 4.13. Then $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$. Since $p \in \mathbb{P}$, $\forall i < p(\gcd(i, p) = 1)$, we can repeatedly apply Theorem 4.14. Therefore $a^{p-1} \equiv 1 \pmod{n}$. ∎

**4.16 Theorem:** In a prime modulo, an integer raised to the power of the modulo is congruent to itself.

Let $p \in \mathbb{P}$ and $a \in \mathbb{Z}$. $a^p \equiv a \pmod{p}$

**Proof:** Let $p \in \mathbb{P}$ and $a \in \mathbb{Z}$. $a^{p-1} \equiv 1 \pmod{p}$ by Theorem 4.15. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$, therefore $a^p \equiv a \pmod{p}$ by Theorem 1.14. On the other hand, if $p|a$, then $a \equiv 0 \equiv a^p \pmod{p}$. Therefore $a^p \equiv a \pmod{p}$ in both cases.

**4.17 Note:** 4.15 and 4.16 are equivalent.

**Proof that 4.15 implies 4.16:** See proof of 4.16 (which relies on 4.15).

**Proof that 4.16 implies 4.15:** Let $p \in \mathbb{P}$ and $a \in \mathbb{Z} \wedge p \nmid a$. $a^p \equiv a \pmod{p}$ by Theorem 4.16. Since $p \in \mathbb{P}$ and $p \nmid a$, $\gcd(a, p) = 1$. This lets us apply Theorem 4.5 to the equation $a^{p-1}a \equiv 1a \pmod{p}$, yielding $a^{p-1} \equiv 1 \pmod{p}$.

**4.18** In a prime modulo, one less than the modulo divides the order of an integer coprime to that modulo.

Let $p \in \mathbb{P}$ and $a \in \mathbb{Z} \wedge p \nmid a$. $\operatorname{ord}_p(a)|(p-1)$

**Proof:** $a^{p-1} \equiv 1 \pmod{p}$ by Theorem 4.15. $(p-1)|\operatorname{ord}_p(a)$ by Theorem 4.10.