Notebook Swag

Sam Grayson

May 20, 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, $\mathrm{pf}(a) \cap \mathrm{pf}(n) = \{\}$. $\min(x\#\,\mathrm{pf}(a), x\#\,\mathrm{pf}(b)) = 0$. 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 $\gcd(a, n) = 1 \to \gcd(a^j, n) = 1$. ■

This proof can also be written using 1.43.

4.3 Theorem: If b is congruent to a coprime of the modulo, then b is a coprime to the modulo.

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: $a^i \equiv a^j \pmod{n}$ Without loss of generality, $i \geq j$. $\frac{a^i}{a^j} \equiv \frac{a^j}{a^j} \pmod{n}$ 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 $\gcd(a, n) = 1 \rightarrow \exists k \in \mathbb{N}(a^k \equiv 1 \pmod{n})$. ∎

4.7 Question: Compute some orders of numbers.

4.8 Theorem: All powers of a relatively prime a up to $\operatorname{ord}_n(a)$ are pair-wise incongruent modulo n.

Translated: $\gcd(a, n) = 1 \wedge i \leq \operatorname{ord}(a) \wedge j \leq \operatorname{ord}(a) \rightarrow a^i \not\equiv a^j$. All congruences and orders are taken to be mod n.

Proof: Assume $a^i \equiv a^j$. Without loss of generality, $i > j$. Then $a^{i-j} \cdot a^j \equiv a^j \cdot 1$ which can be simplified via 4.2 and 4.5 to $a^{i-j} \equiv 1$. But since $\operatorname{ord}(a)$ is the smallest integer with this property, $\operatorname{ord}(a) \leq i - j$. Therefore $i > \operatorname{ord}(a)$. ∎

4.9 Theorem: All powers of a relatively prime a past $\operatorname{ord}_n(a)$ will never produce new numbers mod n.

Translated $i > \operatorname{ord}(a) \rightarrow \exists r \leq \operatorname{ord}(a)(a^i \equiv a^r)$. All congruences and orders are taken mod n.

Proof: Divide i by $\operatorname{ord}(a)$ such that $i = p \cdot \operatorname{ord}(a) + r$ where $0 \leq r < \operatorname{ord}(a)$. $a^i = a^{p \cdot \operatorname{ord}(a) + r} = (a^{\operatorname{ord}(a)})^p \cdot a^r \equiv 1a^r$, or $a^i \equiv 1 \cdot a^r \equiv a^r$. Therefore $i > \operatorname{ord}(a) \rightarrow \exists r \leq \operatorname{ord}(a)(a^i \equiv a^r)$. ∎

4.10 Theorem: $a^m \equiv 1 \leftrightarrow \operatorname{ord}(a)|m$. All congruences and orders are taken mod n.

Proof: $\rightarrow$ Divide m by $\operatorname{ord}(a)$ such that $m = q \cdot \operatorname{ord}(a) + r$ where $0 \leq r < \operatorname{ord}(a)$. $a^m = a^{q \cdot \operatorname{ord}(a) + r} = (a^{\operatorname{ord}(a)})^q \cdot a^r \equiv 1 \cdot a^r$. $\gcd(a^r, n) = 1$, so by Theorem 4.5 $a^r \equiv 1$. But $0 \leq r < \operatorname{ord}(a)$, so $r = 0$. Therefore $m| \operatorname{ord}(a)$.

Proof: $\leftarrow$ $\operatorname{ord}(a)|m$ implies $j \cdot \operatorname{ord}(a) = m$. $a^m = a^{j \cdot \operatorname{ord}(a)} = (a^{\operatorname{ord}(a)})^j \equiv 1^j = 1$.

In conclusion $\operatorname{ord}(a)|m \leftrightarrow a^m \equiv 1$. ∎

4.11 Theorem: The order of a coprime is less than the modulo.

Translated: $\gcd(a, n) = 1 \to \text{ord}(a) < n$. All orders and congruences are taken mod n.

Proof: There can not be more than n unique numbers modulo n by Theorem 3.16. a^i for $0 \leq i < \text{ord}(a)$ produces unique numbers modulo n. Therefore there $\text{ord}(a) < n$. ∎

4.12 Exercise: Compute the following expression for several natural numbers a and prime numbers p $a^{p-1} \pmod p$.

I conjecture that $\text{ord}(a) < n$.

```
def mod_exp(a1, r, n):
    # Returns the k in $a^r \equiv k \pmod n$ where $0 \leq k < r$
    # This algorithm is found in 3.6
    # WLOG a < n
    a = cmod(a1, n) # reduce a mod n if possible
    a_squared = cmod(a * a, n)
    r_halved, remainder = division(r, 2)
    if r == 1:
        # Base case
        return a
    if divides(2, r):
        # $(a^2)^{r/2}$
        k = mod_exp(a_squared, r_halved, n)
        k = cmod(k, n) # reduce k mod n
        return k
    else:
        # $(a^2)^{(r-1)/2} \cdot a$
        k = mod_exp(a_squared, r_halved, n)
        ka = cmod(k * a, n)
        return ka

for p in first(10, primes()):
    print(r'\(\pmod {{{p}}}\)'.format(**locals()))
    print('')
    print(r'\begin{tabular}[t]{l}')
    for a in range(0, p):
        # $0 \leq a < p$
        e = p - 1
        c = mod_exp(a, e, p, False)
        print(r'${a}^{{{e}}} \equiv {c} \pmod {{{p}}}$ \\'.format(**locals()))
    print(r'\end{tabular}')
    print('')
```

Output:

$\pmod 2$

$0^1 \equiv 0 \pmod 2$
$1^1 \equiv 1 \pmod 2$

$\pmod 3$

$0^2 \equiv 0 \pmod 3$
$1^2 \equiv 1 \pmod 3$
$2^2 \equiv 1 \pmod 3$

$\pmod 5$

$0^4 \equiv 0 \pmod 5$
$1^4 \equiv 1 \pmod 5$
$2^4 \equiv 1 \pmod 5$
$3^4 \equiv 1 \pmod 5$
$4^4 \equiv 1 \pmod 5$

⋮

Output has been omitted for brevity.

⋮

$11^{22} \equiv 1 \pmod{23}$
$12^{22} \equiv 1 \pmod{23}$
$13^{22} \equiv 1 \pmod{23}$
$14^{22} \equiv 1 \pmod{23}$
$15^{22} \equiv 1 \pmod{23}$
$16^{22} \equiv 1 \pmod{23}$
$17^{22} \equiv 1 \pmod{23}$
$18^{22} \equiv 1 \pmod{23}$
$19^{22} \equiv 1 \pmod{23}$
$20^{22} \equiv 1 \pmod{23}$
$21^{22} \equiv 1 \pmod{23}$
$22^{22} \equiv 1 \pmod{23}$

What I find interesting is that this program builds off of the one from 3.6. The tools I develop build off of each other. That is the whole idea behind reusable functions in a programming language.

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: (Fermat's Little 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: (Fermat's Little 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 $a \in \mathbb{Z} \wedge p \nmid a$. $\mathrm{ord}_p(a) | (p-1)$

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

4.19 Exercise: Use Fermat's Little Theorem to efficiently raise numbers to large powers in modulo arithmetic.

1. $512^{372} = 512^{31\cdot 12} = (512^{12})^{31} \equiv 1^{31} \pmod{13} = 1$
2. $3444^{3233} = 3444^{202\cdot 16+1} = (344^{16})^{212} \cdot 344^1 \equiv 1^{202} \cdot 344 \pmod{17} = 344$
3. $123^{456} \equiv (2^3)^{456} \pmod{23} = 2^{3\cdot 456} = 2^{62\cdot 22+4} = (2^{22})^{62} \cdot 2^4 \equiv 1^{62} \cdot 2^4 \pmod{23} = 16$

4.20 Exercise: Find the remainder upon division of 314^{159} by 31

$314^{159} \equiv (2^2)^{159} \pmod{31} = 2^{2\cdot 159} = 2^{5\cdot 62+3} = (2^5)^{62} \cdot 2^3 \equiv 1^62 \cdot 2^3 \pmod{31} = 8$

The remainder upon division is $8.2^{144} = (2^{12})^{12} \equiv 1^{12} \pmod 13 = 1$.

4.21 Theorem: $x \equiv a \pmod n$, $x \equiv a \pmod m$, and $\gcd(n, m) = 1$ imply $x \equiv a \pmod{mn}$.

Proof: $n|(x - a)$ and $m|(x - a)$. $mn|(x - a)$ by Theorem 2.25. ■

4.22 Exercise: The remainder of 4^{72} divided by 91 is 8.

$2^{144} = (2^{12})^{12} \equiv 1^{12} \pmod{13} = 1$. Therefore $x \equiv 1 \pmod{13}$

$2^{144} = (2^2)^{72} \equiv 1^{72} \pmod 3 = 1$. Therefore $x \equiv 1 \pmod 3$.

Therefore $4^{72} = 2^{144} \equiv 1 \pmod{91}$ by Theorem 4.21.

4.28 Theorem: $\gcd(a, b) = 1 \wedge \gcd(a, c) = 1 \rightarrow \gcd(a, bc) = 1$

Proof:

Let $\mathrm{pf}(a) = A$, $\mathrm{pf}(b) = B$, $\mathrm{pf}(c) = C$	
$A \cap B = \{\}$	
j $A \cap C = \{\}$	Coprime-disjoint theorem
$\gcd(a, bc) = A \cap (\mathrm{pf}(bc))$	GCD-intersection theorem
$= A \cap (B + C)$	pf of product
$= A \cap B + A \cap C$	Empty-intersection theorem
$= \{\} + \{\}$	Substitution
$= \{\}$	Identity
$\gcd(a, bc) = 1$	Coprime-disjoint theorem ■

4.29 Theorem: 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 $n(c - j) = a$, and then $n|a$, and then $\gcd(a, n) = n$. Therefore $b \neq nc$. Therefore by definition of greatest common divisor $\gcd(b, n) = 1$. In conclusion $(\gcd(a, n) = 1 \wedge b \equiv a \pmod n) \rightarrow \gcd(a, b) = 1$. ■

4.30 Theorem: 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 $a \equiv b \pmod{n}$. ∎

4.31 Theorem: Let $x_1, x_2, \ldots, x_{\phi(n)}$ be the natural numbers relatively prime to n and less than n. Let $\gcd(a, n) = 1$ (but not necessarily $a \leq n$, so not necessarily $\exists i(a = x_i)$). $i \neq j \to ax_i \not\equiv ax_j$

All congruences are taken modulo n.

Proof: $ax_i \equiv ax_j$ implies $x_i \equiv x_j$ by Theorem 4.30, or equivalently $n|(x_i - x_j$. Since $0 \leq x_j < n$ and without loss of generality $x_j \leq x_i < n$, $0 \leq x_i - x_j < n$, but $n|(x_i - x_j)$, therefore $x_i - x_j = 0$. Therefore $x_i = x_j$. This contradicts. Therefore $ax_i \not\equiv ax_j$. ∎

4.32 Theorem: (Euler's Theorem) $a^{\phi(n)} \equiv 1 \pmod{n}$

By Theorem 4.31, the members of the set $\{ax_1, ax_2, \ldots, x_{\phi(n)}\}$ are pairwise incongruent.

4.33 Theorem: (Fermat's Little Theorem) $a^{(p-1)} \equiv 1 \pmod{n}$.

Proof: If $n \in \mathbb{P}$, then all natural numbers less than n are coprime to n. Therefore $\phi(n)$ counts all numbers from 1 to $n - 1$. Therefore $\phi(n) = n - 1$. Therefore $a^{(p-1)} \equiv 1 \pmod{n}$. ∎

4.34 Exercise:

1. $4^{49} \equiv 12^{49} \equiv ? \pmod{15}$
2. $139^{112} \equiv ? \pmod{27}$

4.35 Exercise: Find the ones digit of 13^{474}

$13^{174} = (13^4)^{18} \cdot 13^2 \equiv 1^{18} \cdot 3^2 \pmod{10} = 9$

4.36 Theorem: Every number has a multiplicative inverse in a prime modulo.

Proof: By Fermat's Little Theorem $a^{p-1} \equiv 1$. Since $p \geq 2$, $a^{p-2}a = a^{p-1} \equiv 1$. Therefore reduce a^{p-2} into the CCRS where $a^{p-2} \equiv b$. $\forall 1 < a < p - 1 \exists 1 < b < p - 1 ab \equiv 1$. ∎

4.37 Theorem: 1 and $p - 1$ are their own multiplicative inverses in a prime modulo p.

Translated: $1 \cdot 1 \equiv 1$ and $(p - 1) \cdot (p - 1) \equiv 1$. All congruences are taken mod p

Proof: $1 \cdot 1 = 1 \equiv 1$. $(p - 1) \cdot (p - 1) = p^2 - 2p + 1 = (p - 2) \cdot p + 1 \equiv 1$. ∎

4.38 Theorem: No other number (besides 1 and $p - 1$) is its own inverse in a prime modulo p.

Translated: $0 \leq a < p \wedge a^2 \equiv 1 \to a \equiv 1 \vee a \equiv p - 1$, where all congruences are taken in a prime modulo p.

Proof: Let $a^2 \equiv 1$. By the definition of modulo, $p|(a^2 - 1)$, or equivalently $p|(a - 1)(a + 1)$. $p \in \mathbb{P}$, therefore $\gcd(p, a - 1) = 1$ and $\gcd(p, a + 1) = 1$ (unless $a + 1$ was p or $a - 1$ was 0).

By Theorem 4.28, $\gcd(p, (a-1)(a+1)) = 1$. Therefore $p \nmid (a-1)(a+1$ unless $a = p-1$ or $a = 1$. But we know that $p|(a-1)(a+1)$ from the premise, so $a = p-1$ or $a = 0$. ∎