WORKSHEET 17

Modular Arithmetic

Let m be a positive integer, and let a and b be integers. We say that a *is congruent to* b *modulo* m and write $a \equiv b \pmod{m}$ if $a - b$ is a multiple of m.

PROBLEM 17.1. Show that $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m.

PROBLEM 17.2. Show that there is a unique integer b between 0 and $m-1$ for which $a \equiv b \pmod{m}$.

PROBLEM 17.3. Show that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

PROBLEM 17.4. Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$.

PROBLEM 17.5. Use the previous problem to determine, relatively quickly, what day of the week it was on January 1, 1900. (Make sure you know all the rules for leap years!)

PROBLEM 17.6. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, and $\frac{a}{c}$ and $\frac{b}{d}$ are both integers. Is it necessarily true that $\frac{a}{c} \equiv \frac{b}{d} \pmod{m}$?

PROBLEM 17.7. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Is it necessarily true that $a^c \equiv b^d \pmod{m}$?

PROBLEM 17.8. Is $2222^{5555} + 5555^{2222}$ divisible by 7?

PROBLEM 17.9. You are likely familiar with some divisibility rules:

- A number is divisible by 3 if and only if the sum of its digits is divisible by 3.
- A number is divisible by 9 if and only if the sum of its digits is divisible by 9.
- A number is divisible by 11 if and only if the *alternating* sum of its digits is divisible by 11. (The alternating sum of the digits of $n = a_0 a_1 a_2 \cdots a_k$ is $a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$.)

Explain why all of these are true.

PROBLEM 17.10. For each integer m from 3 to 8, determine those integers b with $0 \leq b \leq m-1$ for which there exists an integer x such that $x^2 \equiv b \pmod{m}$.

PROBLEM 17.11. Show that if $n \equiv 3 \pmod{4}$, then there do not exist two integers x and y such that $x^2 + y^2 = n$.

PROBLEM 17.12. Show that if $n \equiv 7 \pmod{8}$, then there do not exist three integers x, y, and z such that $x^2 + y^2 + z^2 = n$.

DEFINITION. Let p be a prime and let a be an integer. We say that a is a *quadratic residue* modulo p if a is not a multiple of p, and there exists an integer x such that $x^2 \equiv a \pmod{p}$. If there is no integer x such that $x^2 \equiv a \pmod{p}$, then we call a a *quadratic nonresidue* modulo p. We write the symbol $(\frac{a}{p})$ which is 1 if a is a quadratic residue modulo p, -1 if a is a quadratic nonresidue modulo p, and 0 if a is a multiple of p.

PROBLEM 17.13. For how many integers a with $1 \leq a \leq p-1$ is $(\frac{a}{p}) = 1$?

PROBLEM 17.14. Show that $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$.

PROBLEM 17.15. For which primes p is $(\frac{-1}{p}) = 1$? Can you explain why?

PROBLEM 17.16. For which primes p is $(\frac{2}{p}) = 1$? Can you explain why?

Modular Arithmetic

Alexander Friesen 2/24-29/26

17.1: If $a \equiv b \pmod{m}$, then $a-b=km$, where k is any integer. a and b can be expanded to $a=q_1m+r_1$ and $b=q_2m+r_2$ where q is quotient and r is remainder. So, $q_1m+r_1-q_2m-r_2=km$. $r_1-r_2=-q_1m+q_2m+km=m(k-q_1+q_2)$. So r_1-r_2 is a multiple of m. However, both r_1, r_2 and r_1-r_2 must be within the set $[-(m-1), -(m-2), \ldots, -1, 0, 1, \ldots, m-1]$. The only multiple of m in the set of possible remainders is 0, so r_1-r_2 must be 0. Therefore, $r_1=r_2$.

17.2: By the Division Algorithm, for any integer a, $a=qm+r$ and by modular arithmetic $a-b=km$. $a-r=qm$. Let $r=b$ where $0 \leq (r, b) \leq m-1$. Making $q=k$, the two equations become the same, so therefore there will always be a possible integer $0 \leq b \leq m-1$ via this algorithm.

17.3: If $a-b=km$ and $b-c=lm$,
Summing these equations:
$a-b+b-c=km+lm=m(k+1)=a-c$.
So $a-c$ is a multiple of m and $a\equiv c \pmod m$

17.4: Again, $a-b=km$ and $c-d=lm$.

- Add the equations: $a-b+c-d=km+lm=\ldots$
  $\ldots m(k+1)=a+c-(b+d)$. So $a+c\equiv b+d$ is $(\text{mod } m)$.
- Subtract: $a-b-c+d=km-lm=m(k-1)=a-c-(b-d)$
  So $a-c\equiv b-d$ is also $(\text{mod } m)$.
- Multiply: First rearrange so $a=b+km$ and $c=d+qm$.
  Then: $ac=bd+bqm+dkm+kqm^2=bd+m(bq+kd+kmq)$
  So $ac-bd=$ a multiple of m, and $ac\equiv bd \pmod m$.

17.5: Each 365-year taken back from the Wednesday 2025 new year goes back 1 day in the week. 125 days back would take the day of the week to Thursday. There were 31 leap years between 1900 and 2025, so for each extra day of the week shifted back 31 times, it looped to Thurs. 4 times. 31-28=3, so Thurs-3 days = a Monday.

*when divided by 7

17.6: Assume this is true. In that case, divide the 17.4 equations: $\frac{a-b}{c-d} = \frac{km}{lm} = k/l$. Uh-oh, the left side isn't nessecarily a multiple of m anymore! It only is when both k and l are also m-multiples. So $\frac{a}{c} \equiv \frac{b}{d} \pmod m$ isn't always true.

17.7: Take the equation $(a = b + km)^{(c = d + lm)}$.

$a^c = (b+km)^{(d+lm)} = (b+km)^d \cdot (b+km)^{lm}$

$= (b^d + (\text{mod } m)) \cdot (b^{lm} + (\text{mod } m))$.

If $a^c = b^d + (\text{mod } m)$, then this equation would always satisfy. However, this requires that $b^{lm} = 0$. This isn't always true, so the equation isn't always either.

17.8: 2222 and 5555 have remainders 3 and 4 when divided by 7, so now the problem looks like: $3^{5555} + 4^{2222}$.

Powers of 3 repeat remainders* every 6th time, so $5555/6 = R5$, so $3^{5555} \equiv 3^5 \pmod 7$.

Powers of 4 repeat remainders* every... (cont.)

*decrease by 6, not set to -6.

17.8 (cont.): 3rd time, so $\frac{2222}{3} = R2$ and $4^{2222} \equiv 4^2 \pmod 7$. Now the problem is $3^5 + 4^2$. Calculating this gives 259, which divided by 7 equals 37. So $2222^{5555} + 5555^{2222}$ is mod 7.

17.9: ÷3 Rule: Say there is a number n, divisible by 3, that also has a sum of digits div. by 3. If n+3 also has a sum of digits div. by 3, then by induction the rule is true. Either:

- The sum of digits increases by 3
- The +3 carries over, making the sum of digits $-9+3 = -6$.*

(For a hundreds/thousands/etc. carryover, minus an extra 9.)

Both of these results keep n's digit sum divisible by 3, so the rule always works.

÷9 Rule: Same thing, but either sum of digits +9 or +0 or -9... still works...

*Each 10^n is 1 more or less than a mult. 11.

17.9 (cont.): ...÷11 Rule: Say we have an x-digit number (my example x=4), abcd. Expanded form is 1000a+100b+10c+d. Rewritten to include multiples of 11*: 1001a-a+99b+b+11c-c+d. Factor multiples of 11 out: 11(91a+9b+c)+(-a+b-c+d). The left term is a multiple of 11, so the right term must be too for abcd to be a mult. 11. The right term, -a+b-c+d, is where the alternating sum comes from.

17.10: m=3 b=0: Yes, x=9. b=1: Yes, x=4. b=2: No. m=4 b=0: Yes, x=8. b=1: Yes, x=5. b=2: No. b=3: No. m=5 b=0: Yes, x=5. b=1: Yes, x=6. b=2: No. b=3: No. b=4: Yes, x=7. m=6 b=0: Yes, x=6. b=1: Yes, x=5. b=2: No. b=3: Yes, x=9. b=4: Yes, x=4. b=5: No. m=7 b=0: Yes, x=7. (cont.)

*summing only 0s and 1's can yield 0, 1, or 2.

17.10 (cont.): b=1: Yes, x=8. b=2: Yes, x=3.
b=3: No. b=4: Yes, x=5. b=5: No. b=6: No.
m=8 b=0: Yes, x=8. b=1: Yes, x=7. b=2: No.
b=3: No. b=4: Yes, x=6. b=5: No. b=6: No.
b=7: No. (These b-values are "quadratic residue.")

17.11: Two cases: x is even or x is odd.
Even: x^2 contains 2 factors of 2
and therefore is in mod 4.
Odd: $x^2-1=(x+1)(x-1)$, both each even.
So x^2 is one more than a mod 4
number ($x^2 \equiv 1 \pmod 4$.)
In both cases, $x^2 \equiv [0,1] \pmod 4$.
Adding another square allows
$(x^2+y^2) \equiv [0,1,2] \pmod 4$,* but not
$3 \pmod 4$.

17.12: Again, two cases, even or odd.
Even: $0^2=0$, $2^2=4$, $4^2=0 \pmod 8$, $6^2=4 \pmod 8$.
All even remainders yield residues $[0,4]$.
Odd: $1^2=1$, $3^2=1 \pmod 8$, $5^2=1 \pmod 8$, etc.
All odd remainders have residue(s) 1.
No combination of 0, 4, or 1 adds up to $7 \pmod 8$.

*The new "half set," which is $(1^2, 2^2, \ldots, (\frac{p-1}{2})^2)$.

17.13: For any prime mod p, the entire set of possible residues is the squares of all integers under p: $(1^2, 2^2, \ldots, (p-1)^2)$. Because each square can be mapped to both a + and − root, only exactly half of the set of squares must be considered to avoid duplicates. The size of this set is $\frac{p-1}{2}$*.

17.14: Write out $\frac{a}{p}$ and $\frac{b}{p}$ as: $x^2 - a = kp$ and $y^2 - b = lp$. Multiply the equations together: $(x^2-a)(y^2-b) = klp^2$ $= x^2y^2 + ab - x^2b - y^2a$. This equation includes ab and entirely square factors equalling a multiple of p, so $\frac{ab}{p}$ corresponds to $(\frac{a}{p})(\frac{b}{p})$.

Not sure on the Proofs for these.

17.15: Some primes that work are 2 ($1^2+1 \equiv 2 \pmod 2$) and any prime satisfying $p \equiv 1 \pmod 4$ ($2^2+1 \equiv 5 \pmod 5$).

17.16: Some solutions are 2, $p \equiv 1 \pmod 8$ ($6^2 - 2 \equiv 0 \pmod{17}$), and $p \equiv 7 \pmod 8$ ($3^2 - 2 \equiv 0 \pmod 7$).