Name: Solutions

Directions: Show all work unless directed otherwise. No credit for answers without work.

1. **[5 points]** Short Answer. Jesse and Marie use a simple Caeser cipher to exchange secret messages in social studies class. (They would never do such a thing in their mathematics classes.) You hear Jesse boast that their secret key k is the best possible key since it makes the processes of encoding and decoding exactly the same. Assuming that their encryption scheme is non-trivial (i.e. $k \neq 0$), what is k?

   $k = 13$. (Mod 26, adding ~~k~~ 13 and subtracting 13 is the Same.)

2. **[10 points]** Is the following statement true or false? Let a, b, and c be integers. If $a \mid b + c$, then $a \mid b$ and $a \mid c$. If the statement is true, give a proof. If the statement is false, give a counterexample (that is, a specific example of particular integers a, b, and c for which the statement fails).

   False For example, if $a=5$, $b=7$, and $c=3$,

   then

   $5 \mid 7+3$ but $5 \nmid 7$ and $5 \nmid 3$.

3. **[5 points]** Find the quotient q and remainder r that results from dividing -308 by 86.

   $-308 = (-4)(86) + 36$, so

   $\boxed{q = -4 \text{ and } r = 36}$.

4. **[5 points]** Give 3 different examples of integers that are congruent to 79 modulo 145. If possible, one of your examples should be negative.

   $\boxed{79}$ $79 - 145$ or $\boxed{-66}$

   $79 + 145$ or $\boxed{224}$.

5. Proofs.

   (a) **[15 points]** Let a and b be integers. Prove that if there exist integers u and v such that $ua + vb = 1$, then $\gcd(a, b) = 1$.

Note that a and b cannot both be zero, or else u and v would not exist. Let $d = \gcd(a,b)$. Since $d \mid a$ and $d \mid b$, it follows that $d \mid ua+vb$, and therefore $d \mid 1$. The only divisors of 1 are +1 and −1.

Since the greatest common divisor is always positive, it follows that $d = 1$.

   (b) **[15 points]** Let x and y be integers, not both zero, and let $d = \gcd(x, y)$. Prove that $\gcd(\frac{x}{d}, \frac{y}{d}) = 1$.

Since $d = \gcd(x,y)$, there exist integers u and v such that $ux + vy = d$. Dividing both sides by d, we see that

$$u\frac{x}{d} + v\frac{y}{d} = 1.$$

By part (a) with $a = \frac{x}{d}$ and $b = \frac{y}{d}$, it follows that $\gcd(\frac{x}{d}, \frac{y}{d}) = 1$.

6. **[20 points]** Use the extended Euclidean algorithm to find gcd(28543, 32147) and express it as an integer combination of 28543 and 32147.

$$32147 = (1)\,28543 + 3604$$

$$28543 = (7)\,3604 + 3315$$

$$3604 = (1)\,3315 + 289$$

$$3315 = (11)\,289 + 136$$

$$289 = (2)\,136 + 17$$

$$136 = (8)\,17 + 0.$$

So $\gcd(32147, 28543) = \gcd(17, 0) = \boxed{17}$.

$$17 = (1)(289) - (2)(136)$$

$$= (1)(289) - (2)\left[3315 - (11)289\right]$$

$$= (23)(289) - (2)(3315)$$

$$= (23)\left[3604 - (1)3315\right] - 2(3315) = (23)(3604) - (25)(3315)$$

$$= (23)(3604) - (25)\left[28543 - (7)3604\right] = (198)(3604) - (25)(28543)$$

$$= (198)\left[32147 - (1)28543\right] - (25)(28543)$$

$$= (198)(32147) - (223)(28543)$$

7. **[15 points]** Solve for x in $424x \equiv 19 \pmod{643}$.

Find a mult. inverse for 424:

$$643 = (1)(424) + 219$$
$$424 = (1)219 + 205$$
$$219 = (1)205 + 14$$
$$205 = (14)14 + 9$$
$$14 = (1)9 + 5$$
$$9 = (1)5 + 4$$
$$5 = (1)4 + 1$$

$$1 = 5 - (1)4$$
$$= 5 - (1)[9 - (1)5]$$
$$= (2)5 - (1)9 = (2)[14 - (1)9] - (1)9$$
$$= (2)14 - (3)9$$
$$= (2)14 - (3)[205 - (14)(14)]$$
$$= (44)(14) - 3(205) = (44)[219 - 205] - 3(205)$$
$$= (44)(219) - (47)(205)$$
$$= (44)(219) - (47)(424 - (1)(219))$$
$$= (91)(219) - (47)(424)$$
$$= (91)[643 - (1)424] - (47)(424)$$
$$= (91)(643) - (138)(424).$$

So, inverse is -138.

$$424x \equiv 19$$
$$(-138)424x \equiv (-138)(19)$$
$$x \equiv -2622 \equiv \boxed{593}$$

8. The group of units.

(a) **[5 points]** Give the multiplication table for $\mathbb{Z}_{10}^*$.

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(b) **[5 points]** What is $\phi(10)$?

$$\phi(10) = |\mathbb{Z}_{10}^*| = \boxed{4}$$