A1. Use the extended Euclidean algorithm to verify that $\gcd(427, 2818) = 1$ and to find the multiplicative inverse of 427 modulo 2818.

Solution: Solution: We get

$$\begin{aligned} 2818 &= 6 \times 427 + 256 \\ 427 &= 1 \times 256 + 171 \\ 256 &= 1 \times 171 + 85 \\ 171 &= 2 \times 85 + 1 \end{aligned}$$

Now we use back-substitution to get

$$\begin{aligned} 1 &= 171 - 2 \times 85 \\ &= 171 - 2(256 - 171) \\ &= -2 \times 256 + 3 \times 171 \\ &= -2 \times 256 + 3(427 - 256) \\ &= 3 \times 427 - 5 \times 256 \\ &= 3 \times 427 - 5(2818 - 6 \times 427) \\ &= -5 \times 2818 + 33 \times 427. \end{aligned}$$

Thus $427 \times 33 \equiv 1 \pmod{2818}$.

A2. Agent Jayne Bond encrypts a number a (with $0 \leq a \leq 2818$) by raising a to the power 427 and reducing the result modulo the prime 2819. She reports that the encrypted version of a is 1268. What was a?

Solution: By Fermat's little theorem, we know that $(a^{427})^{33}$ is congruent to a modulo 2819, so we need to raise 1268 to the power 33 modulo 2819. We compute

$$\begin{aligned} 1268^1 &\equiv 1268 \pmod{2819} \\ 1268^2 &\equiv 994 \pmod{2819} \\ 1268^4 &\equiv 1386 \pmod{2819} \\ 1268^8 &\equiv 1257 \pmod{2819} \\ 1268^{16} &\equiv 1409 \pmod{2819} \\ 1268^{32} &\equiv 705 \pmod{2819} \end{aligned}$$

Then

$$\begin{aligned} 1268^{33} &\equiv 1268 \times 1268^{32} \pmod{2819} \\ &\equiv 1268 \times 705 \pmod{2819} \\ &\equiv 317 \pmod{2819} \end{aligned}$$

The value of a was 317.

A3. Agent Bond uses the same scheme to encrypt five more numbers between 0 and 2818 (inclusive), and reports the results: 468, 2685, 1088, 2684, and 2424. She claims that the six numbers she's sent us spell an *alphabetic* message. What is it?

Solution: We use a POWERMOD program on our calculator to compute

$$\begin{aligned} 468^{33} \bmod 2819 &= 2415 \\ 2685^{33} \bmod 2819 &= 1914 \\ 1088^{33} \bmod 2819 &= 1514 \\ 2684^{33} \bmod 2819 &= 2204 \\ 2424^{33} \bmod 2819 &= 1700 \end{aligned}$$

The string of numbers we have is

$$0317, 2415, 1914, 1514, 2204, 1700.$$

Each pair of digits can be read as a number between 0 and 25, so we suspect Agent Bond might have used the usual alphabetic translation $0 =$ `A`, $1 =$ `B`, and so on. Using this idea, we read

`DRYPTOPOWERA`.

It doesn't make much sense, but at least it's pronounceable. Perhaps the final `A` is just filler, and the message is "`DRYPTOPOWER`." That's kind of silly, too. Perhaps Agent Bond meant to send "cryptopower," and mis-encrypted the first letter. Or maybe she was just in a bad mood.

B1. We are given that the numbers 2063 and 3779 are prime and that

$$2063 \times 3779 = 7796077.$$

Find the smallest exponent $e \geq 2$ such that

$$a^e \equiv a \pmod{7796077}$$

for every integer a.

Solution: By Euler's generlization to Fermat's little theorem, we know that $a^e \equiv a \pmod{pq}$ for every a if $e \equiv 1 \pmod{(p-1)(q-1)}$.

In this case, $p-1 = 2062$ and $q-1 = 3778$, so $(p-1)(q-1) = 7790236$. The smallest number (≥ 2) that's congruent to 1 modulo 7790236 is 7790237.

That's the smallest number that Euler's generalization gives us, and it's an acceptable answer.

But it's not quite correct. Using a little number theory (which we haven't seen in this course), we can find a smaller value for e. Here's how:

The statement "$a^e \equiv a \pmod{2063 \times 3779}$ for every a" is equivalent to the statement "$a^e \equiv a \pmod{2063}$ and $a^e \equiv a \pmod{3779}$ for every a." Now 2063 and 3779 are primes, and we know (from a number theory book), that if $a^e \equiv a \pmod{p}$ for a prime p, then e *must* be congruent to 1 modulo $p-1$. (The fancy way to say this is "primes have primitive roots.") So the e that we're looking for must be congruent to 1 modulo 2062 and congruent to 1 modulo 3778.

That is, $e-1$ must be divisible by both 2062 and 3778, so it must be divisible by their least common multiple. The prime factorizations of 2062 and 3778 are 2×1031 and 2×1889 respectively, so their least common multiple is $2 \times 1031 \times 1889 = 3895118$. Now we know that $e-1$ must be divisible by 3895118.

Set $e = 3895119$. Then e is one more than a multiple of 2062 and one more than a multiple of 3778. By Fermat's little theorem, then, $a^e \equiv a \pmod{2063}$ for all a, and $a^e \equiv a \pmod{3779}$ for all a. This means that $a^e - a$ is divisble by both 2063 and 3779 for every a, and since 2063 and 3779 are prime, $a^e - a$ must be divisible by their product, 796077.

We have proved that $e = 3895119$ is the least exponent (≥ 2) for which $a^e \equiv a \pmod{7796077}$ for all a.

B2. An important phone number has been encrypted for us by raising it to the power 4232091 and reducing the result modulo 7796077. The encrypted phone number is 2046049. What was the original phone number?

Solution: We need the decryption exponent, which is

$$4232091^{-1} \pmod{7790236}$$

Using the extended Euclidean algorithm program on line, we find that

$$1075 \times 4232091 - 584 \times 7790236 \quad = \quad 1,$$

so our decryption exponent is 1075. Next we use the on-line Powermod calculator to find that

$$2046049^{1075} \text{ MOD } 7796077 \quad = \quad 5682267.$$

This turns out to be the phone number of the automated weather information service at Barnes/Westfield airport.

B3. Our adversary is encrypting numbers between 1 and 50 by raising them to some power k and reducing the result modulo some prime p. By interviewing one of the adversary's agents, we discover that he is using $p = 53$.

(a) What are the possible values for k?

Solution: Since k must be relatively prime to $p - 1 = 52$, we know it cannot be any multiple of 2 or 13. The possiblities are

$$1, 3, 5, 7, 9, 11, 15, 17, 19,$$
$$21, 23, 25, 27, 29, 31, 33, 35, 37,$$
$$41, 43, 45, 47, 49, 51.$$

(b) In an effort to discover k, we trick our adversary into encrypting a known number. He encrypts the number 23, and the result is 30. What can we deduce about k from this crib?

Solution: Since $23^4 \equiv 1 \pmod{53}$ and $23^3 \equiv 30 \pmod{53}$, we know that $k \equiv 3 \pmod{4}$. This narrows down the possibilities for k to the list 3, 7, 11, 15, 23, 27, 31, 35, 43, 47, 51.

(c) Through a lucky accident, we get one more crib: our adversary encrypts the number 10 and gets the result 28. What do we know now about the number k?

Solution: Now k has to be 9 or 35, so we know it's 35.