Entirely by hand:

$$5^{13} \pmod{23}$$

$$5^1 \equiv 5 \pmod{23}$$
$$5^2 \equiv 2 \pmod{23}$$
$$5^4 \equiv 4 \pmod{23}$$
$$5^8 \equiv 1 \pmod{23}$$
$$5^{13} \equiv 5^8 \cdot 5^4 \cdot 5^1 \equiv 16 \cdot 4 \cdot 5 \equiv 16 \cdot 20 \equiv -7 \cdot -3 \equiv 21 \pmod{23}.$$ 

So $$5^{13} \equiv 21 \pmod{23}.$$ 

$$28 \equiv 28 \pmod{1147}$$

[with 4-function calculator]

$$28 \equiv 28 \pmod{1147}$$
$$28^2 \equiv 784 \pmod{1147}$$
$$28^4 \equiv 1011 \pmod{1147}$$
$$28^8 \equiv (-136)^2 \equiv 144 \pmod{1147}$$
$$28^{16} \equiv 90 \pmod{1147}$$
$$28^{32} \equiv 71 \pmod{1147}$$
$$28^{64} \equiv 453 \pmod{1147}$$
$$28^{128} \equiv 1043 \pmod{1147}$$
$$28^{256} \equiv 493 \pmod{1147}$$
$$28^{512} \equiv 1032 \pmod{1147}.$$ 

$$28^{249} \equiv 28 \pmod{1147}.$$ 

$$\Rightarrow 28^{249} \equiv 28 \pmod{1147}.$$
Note \( 1147 = 3 \cdot 37 \), so \( \phi(1147) = 30 \cdot 36 = 1080 \).

We want a solution to \( 329u - 1080v = 1 \).

Using the Euclidean algorithm, we see \( v = 929 \) is a solution.

Then \( x = 452 \cdot 929 \equiv 763 \pmod{1147} \) is the solution.

17.2 463 is prime, and \( \phi(463) = 462 \).

\[ 113u - 462v = 1 \quad \text{has \( v = 323 \) as a solution.} \]

Then \( 347 \cdot 323 \equiv 37 \pmod{463} \) is a solution.

For \( b \), the solution is \( 139 \cdot 559 \equiv 1 \pmod{588} \).

17.5 (a) To solve \( x^2 \equiv 23 \pmod{1279} \), we would try to solve \( 2u - 1278v = 1 \). But this has no solution.

(b) As \( \phi(p) \) is even for odd primes, this always happens for odd primes + square roots.

(c) Generally, if we cannot solve \( kv - clcmv = 1 \), then this methodology does not work.
Using the Euclidean Algorithm, one solves

\[ u \cdot 1789 - v \cdot 6912 = 1 \]

and finds \( u = 85 \).

Now, to decode:

Take \( 5192 \quad 85 \equiv 1615 \mod 7081 \)

\[ 2604 \quad 85 \equiv 2823 \mod 7081 \]

\[ 4227 \quad 85 \equiv 1130 \mod 7081 \]

Add \( 1615 \ 2823 \ 1130 \rightarrow \text{FERMAT} \).

So the secret message is \text{Fermat}. \&
Suppose that \( a \) is our message, and suppose
\[ M = p_1p_2 \ldots p_r \]
is a product of distinct primes.

Then we want to show that, given \( k \) with
\[ \gcd(k, \text{lcm}) = 1 \]
(so that we can find \( u \), a solution to \( uk - v \text{lcm} = 1 \)),
then \( a^k = a \pmod{m} \), even if \( \gcd(a, m) > 1 \).

Equivalently, we need to check that \( m \mid ku \)
We do this in the spirit of the Chinese Remainder Theorem,
by showing \( p_i \mid ku \) for each \( p_i \mid m \).

Note that \( \text{lcm} = (p_1 - 1)(p_2 - 2) \ldots (p_r - 1) \), so \( (p_i - 1) \mid \text{lcm} \).
Then
\[ ku \equiv 1 + v \text{lcm} \pmod{p_i} \]
\[ a = a \pmod{p_i} \].
If \( p_i \nmid a \), then clearly
\[ p_i \nmid a - a \]. Otherwise, by CRT, we have
\[ ku \equiv 1 + v \text{lcm} \pmod{p_i} \]
\[ a = a \equiv a \pmod{p_i} \]
so that \( p_i \nmid a - a \) still. As this is true for each
\( p_i \mid m \), by the CRT we have \( m \mid ku \)
and so RSA works for all messages \( a \) as long as \( m \) is a product
of distinct primes.