Homework #7 Solutions

16.1 Entirely by hand:

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

$5^1 \equiv 5 \quad (23)$

$5^2 \equiv 2 \quad (23)$

$5^4 \equiv 4 \quad (23)$

$5^8 \equiv 16 \quad (23)$

$5^{13} \equiv 5^8 \cdot 5^4 \cdot 5^1 \equiv 16 \cdot 4 \cdot 5$

$\equiv 16 \cdot 20 \equiv -7 \cdot -3 \equiv 21 \ (23).$

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

$28^{749} \pmod{1147}$ [with 4-function calculator]

$28 \equiv 28 \quad (1147)$

$28^2 \equiv 784 \quad (1147)$

$28^4 \equiv 1011 \quad (1147)$

$28^8 \equiv (-136)^2 \equiv 144 \quad (1147)$

$28^{16} \equiv 90 \quad (1147)$

$28^{32} \equiv 71 \quad (1147)$

$28^{64} \equiv 453 \quad (1147)$

$28^{128} \equiv 1043 \quad (1147)$

$28^{256} \equiv 493 \quad (1147)$

$28^{512} \equiv 1032 \quad (1147)$

$\Longrightarrow \quad 28^{749} \pmod{1147}$

is $28^{512}\, 28^{128}\, 28^{64}\, 28^{32}\, 28^{8}\, 28^{4}\, 28$

$\equiv 289 \bmod 1147.$

$\blacksquare$

$\boxed{17.1}$ Note $1147 = 31 \cdot 37$, so $\varphi(1147) = 30 \cdot 36 = 1080$.

We want a solution to $329u - 1080v = 1$.
Using the Euclidean Algorithm, we see $u = 929$ is a solution.

Then $x \equiv 452^{929} \equiv 763 \pmod{1147}$ is the solution. ∎

$\boxed{17.2}$ 463 is prime, and $\phi(463) = 462$.

$113u - 462v = 1$ has $u = 323$ as a solution.

Then $347^{323} \equiv 37\ (463)$ is a solution

For b, the solution is $139^{11} \equiv 559 \pmod{588}$. ∎

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

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

(c) Generally, if we cannot solve $ku - \varphi(m)v = 1$, then this methodology does not work. ∎

$\boxed{18.1}$ $7081 = 73 \cdot 97$, so $\varphi(7081) = 72 \cdot 96 = 6912$.

Using the Euclidean Algorithm, one solves

$$u \cdot 1789 - v \cdot 6912 = 1$$

and finds $u = 85$.

Now, to decode:

take $5192^{85} \equiv 1615 \mod 7081$

$2604^{85} \equiv 2823 \mod 7081$

$4222^{85} \equiv 1130 \mod 7081$

And $1615\ 2823\ 1130 \longmapsto$ FE RM AT.

So the secret message is Fermat. $\blacksquare$

18.2 Suppose that a is our message, and suppose

$m = p_1 p_2 \cdots p_\ell$ is a product of distinct primes.

Then we want to show that; given k with

$\gcd(k, \varphi(m)) = 1$ (so that we can find u, a

solution to $uk - v\varphi(m) = 1$),

then $(a^k)^u \equiv a \pmod{m}$, even if $\gcd(a,m) > 1$.

Equivalently, we need to check that $m \mid a^{ku} - a$.
We do this in the spirit of the Chinese Remainder Theorem,
by showing $p_i \mid a^{ku} - a$ for each $p_i \mid m$.

Note that $\varphi(m) = (p_1 - 1)(p_2 - 1) \cdots (p_\ell - 1)$, so $(p_i - 1) \mid \varphi(m)$.

Then $a^{ku} = a^{1 + v\varphi(m)}$. If $p_i \mid a$, then clearly

$p_i \mid a^{ku} - a$. Otherwise, by FLT, we have

$$a^{ku} = a^{1 + v\varphi(m)} \equiv a \cdot a^{(p_i - 1)\left(\frac{v\varphi(m)}{p_i - 1}\right)} \equiv a \mod p_i,$$

so that $p_i \mid a^{ku} - a$ still. As this is true for each

$p_i \mid m$, by the CRT we have $m \mid a^{ku} - a$, and

so RSA works for all messages a as long as m is a product

of distinct primes. ∎