1. Express gcd(4321, 3456) as

$4321x + 3456y$

	x	y	4
4321	1	0	
3456	0	1	
865	1	-1	1
861	-3	4	3
4	4	-5	1
1	-863	1079	215

$1 = -863 * 4321 + 1079 * 3456$

(2) $N = 91 = 7 \cdot 13$

$r = 5$

I didn't chose 3 because $\gcd(3, 6 \cdot 12) \neq 1$

$s = 5^{-1} \bmod 72$

72	1	0	
5	0	1	
2	1	-14	14
1	-2	29	2

$s = 5^{-1} \bmod 72 = 29.$

$35^{29} \bmod 91$ is what we seek

29	$42^2 \cdot 35 \bmod 91 = \boxed{42}$
14	$35^{2} \bmod 91 = 42$
7	$14^2 \cdot 35 \bmod 91 = 35$
3	$35^3 \bmod 91 = 14$
1	35

35 is not relatively prime to 91!

$\gcd(35, 91) = 7$?

a

(3) How many generators are there in mod 29 arithmetic?

By PRT, ~~gcd~~ there are $\phi(28)$ generators.

$$\phi(28) = \phi(4)\cdot\phi(7) = 2\cdot 6 = 12$$

2 is a generator

2
4
8
16
3 $16*2-29$
6
12
24
19
9
18
7
14
28 ← you already had it
29

is a generator here.
it is of order > 14
so it is of order 28.

(4) determine whether 2435 is a QR mod 2801 by calculating Legendre symbols

$$\left(\frac{2435}{2801}\right) = \left(\frac{2801}{2435}\right) = \left(\frac{366}{2435}\right) = \underbrace{\left(\frac{2}{2435}\right)}_{-1}\left(\frac{183}{2435}\right)$$

$2435 \equiv_8 3$

$$(-1)(-1)\left(\frac{2435}{183}\right) = (-1)(-1)\left(\frac{56}{183}\right) = (-1)(-1)\left(\frac{8}{183}\right)\left(\frac{7}{183}\right)$$

$$= (-1)(-1)\underbrace{\left(\frac{2}{183}\right)}_{1}(-1)\left(\frac{183}{7}\right)$$

$183 \equiv_8 -1$

$$= (-1)(-1)(1)(-1)(1) = -1$$

5) find a, b st

$$a^2 + b^2 = 157$$

$$129^2 + 1^2 = (106)(157) \quad g \text{ mes}$$

$A = 129$ $\quad m = 106$

$B = 1$ $\quad p = 157$

$u = 129 - 106 = 23$

$v = 1$

$$\frac{uA + vB}{m} = 28 \qquad \frac{vA - uB}{m} = 1$$

now $\quad 28^2 + 1^2 = 5(157)$

$A = 28 \quad B = 1 \quad m = 5$

silly mes → $\quad u = 3 \quad v = 1$

u should be -2 but my calc does work

$$\frac{uA + vB}{m} = 17 \qquad \frac{vA - uB}{m} = 5$$

$$17^2 + 5^2 = 2(157)$$

$m = 2$

$u = 1 \quad v = 1$

$$\frac{17+5}{2} = 11 \qquad \frac{17-5}{2} = 6$$

$$\boxed{11^2 + 6^2 = 157}$$

(6) Prove that if $2^p - 1$ is prime then

$$x = 2^{p-1}(2^p - 1) \text{ is perfect}$$

$$\sigma\left(2^{p-1}(2^p - 1)\right) =$$

$$\sigma(2^{p-1})\,\sigma(2^p - 1)$$

2^{p-1} and $2^p - 1$ are relatively prime because $2^p - 1$ is odd

Sum of geometric series

$$= (2^p - 1)\left((2^p - 1) + 1\right)$$

because $2^p - 1$ is prime

$$\sigma(x) = 2^p(2^p - 1) = 2\left(2^{p-1}(2^p - 1)\right) = 2x$$

so it is perfect.

7. Show that if $\gcd(b,m)=1$ and $\gcd(k,\phi(m))=1$ then b has one and only one kth root in ~~mod~~ mod m arithmetic

for some u, v: $ku+\phi(m)v=1$

$\cancel{b^u} \equiv \cancel{b^{ku}}$

$$(b^u)^k \equiv_m b^{ku} \equiv_m (b^{ku})(b^{\phi(m)v}) \equiv_m \cancel{b^{ku}} \; b^{ku+\phi(m)v} \equiv_m b!$$

euler's thm, $b^{\phi(m)} \equiv 1$

so b^u is a kth root.

Now suppose $x^k \equiv_m b$ mod m — $\gcd(x,m)=1$ hold here otherwise x^k could not be b - $\gcd(x^k)$ would not be 1 for any k,

then $x^{ku} \equiv_m b^u$

and $x^{ku} \equiv x^{ku+\phi(m)v} \equiv x$

so $x \equiv_m b^u$, x is the kth root we already know about.

(8) Prove the Rabin-Miller Theorem:

If p is an odd prime and $0 < a < p$

and $p-1 = 2^k q$, q odd

then either $a^q \equiv 1 \bmod p$ or some $a^{2^i q} \equiv -1 \bmod p$

where $0 \leq i < k$. You need ~~the~~ FLT and

a fact about roots of polynomials in prime moduli.

We know that $a^{2^k q} \equiv 1 \bmod p$ by the FLT

$(a^{p-1} \equiv 1 \bmod p)$

so there is a first i such that $a^{2^i q} \equiv 1 \bmod p$

if $i = 0$ we have ~~a~~ $a^q \equiv 1 \bmod p$

otherwise $i = j+1$ and we have $(a^{2^j q})^2 \equiv 1 \bmod p$

but $a^{2^j q} \not\equiv 1 \bmod p$. By Polynomial Roots Theorem

(name?) $x^2 \equiv 1 \bmod p$ has only two roots, -1 and 1.

So $a^{2^j q} \equiv -1 \bmod p$.

So we have either $a^q \equiv 1 \bmod p$ or $a^{2^j q} \equiv -1 \bmod p$

for some j.

with $0 \leq j < k$

by construction