1) $13^{650} \bmod 151$

$650_{10} = 1010001010_2$ // base 2

512	256	128	64	32	16	8	4	2	1
1	0	1	0	0	0	1	0	1	0

if ($base_2 \bmod 2 \equiv 1$)
  $answer *= base^{Power} \bmod m$
  $base_2 -= 1$

$base_2 /= 2$
$Power *= 2$

$base^{Power}$ can be calculated by:

```
for(i=0; i<Power; i++)
  base *= power
  base = base mod m
```

Power	m	$base_2$	base	answer work	answer	
1	151	1010001010	13	1		0 mod 2 ≡ 0
2		101000101		$1 * 13^2 \% 151$	18	1 mod 2 ≡ 1
4		10100010			18	0 mod 2 ≡ 0
8		1010001		$18 \cdot 13^8 \% 151 =$	105	1 mod 2 ≡ 1
16		101000			105	0 mod 2 ≡ 0
32		10100			105	0 mod 2 ≡ 0
64		1010			105	0 mod 2 ≡ 0
128		101		$105 \cdot 13^{128} \% 151 =$	91	1 mod 2 ≡ 1
256		10			91	0 mod 2 ≡ 0
512		1		$91 \cdot 13^{512} \% 151 =$	118	1 mod 2 ≡ 1

2) $\begin{cases} x \equiv 21 \bmod 29 & x = 21 + 29i \\ x \equiv 17 \bmod 41 & x = 17 + 41k \\ x \equiv 3 \bmod 79 & x = 3 + 79m \end{cases}$ $\gcd(29, 41, 79) = 1$

b	m	W	p	x^{-1}	$\prod b n x^{-1}$
21	29		3239	17	1156323
17	41	74497	1817	19	596891
3	79		943	63	178227

$\Sigma = 1921141141 \equiv N \equiv 59016 \% 74497$

59016 mod 74497

2b) $\{13 \bmod 85, 78 \bmod 95, 97 \bmod 437\}$ $\gcd = 5, 19$ $\}=1$

$13 \bmod 17$	$13 \bmod 17$
$13 \bmod 5$	$3 \bmod 5$
$78 \bmod 19$	$2 \bmod 19$
~~$78 \bmod 5$~~	
$97 \bmod 23$	$5 \bmod 23$
~~$97 \bmod 19$~~	

chineseRem$\left(\begin{bmatrix} 13 & 17 \\ 3 & 5 \\ 2 & 19 \\ 5 & 23 \end{bmatrix}\right) = 34183 \bmod 37145$

3) Find all $x \in \mathbb{Z} \mid 3000 < x < 5000$

$$x \equiv 1 \bmod 7$$
$$x \equiv 3 \bmod 11$$
$$x \equiv 5 \bmod 13$$

$x \equiv 421 \bmod 1001$

$x + 1001 \equiv x \ldots$

3000 5000

421 1422 2423 | 3424 4425 | 5426

3424 and 4425

4) $x + 2y + 3z \equiv 1 \pmod{11}$
$x + 2y + 5z \equiv 4$
$7x + 3y + z \equiv 10$

$$\begin{bmatrix} 1 & 2 & 3 & 1 \\ 1 & 2 & 5 & 4 \\ 7 & 3 & 1 & 10 \end{bmatrix} R_2 + 3R_3 \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & 0 & 8 & 1 \\ 7 & 3 & 1 & 10 \end{bmatrix} R_3 + 4R_1 \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & 0 & 8 & 1 \\ 0 & 0 & 2 & 3 \end{bmatrix} R_3 * 6 \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & 0 & 8 & 1 \\ 0 & 0 & 1 & 7 \end{bmatrix}$$

$$R_2 + 3R_3 \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 \end{bmatrix}$$

$x+2y+3(7) \equiv 1$
$x+2y+5(7) \equiv 4$
$7x+3y+(7) \equiv 10$

$x+2y \equiv 2 \pmod{11}$
~~$x+2y \equiv 2$~~
$7x+3y \equiv 3$

$x \equiv 2+9y \bmod 11$
$y \equiv y \bmod 11$
$z \equiv 7 \bmod 11$

5) Count factors of 7 in 2500!

$$\left\lfloor \frac{2500}{7} \right\rfloor + \left\lfloor \frac{2500}{7^2} \right\rfloor + \left\lfloor \frac{2500}{7^3} \right\rfloor = 357+51+7 = 415$$

415

5b) Count 7 factors in $\frac{2500!}{500!}$

$$\frac{2500!}{500!} = \frac{2500 \cdot 2499 \ldots}{500 \cdot 499 \ldots} = \prod_{501}^{2500} k$$

factors of 7 in $2500 = 415$
$500 = 82$

So factors in $\frac{2500!}{500!}$ should be $415-82 = 333$

1 2 1 | 1 1 1 | 8 4 2 1

$\ldots 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$
(Some huge #) $5 \cdot 4 \cdot 3 \cdot 2$

factors 2 for example

333

6) $N \mid N!$ ends with 100 0's

ie Count of 5 factors = 100

$$\left\lfloor \frac{N}{5} \right\rfloor + \left\lfloor \frac{N}{5^2} \right\rfloor + \left\lfloor \frac{N}{5^3} \right\rfloor \ldots = 100$$

$5^4 = 625$ There are more than 100 factors So too big

125 has 31 factors
25 has 6 factors = $31x + 6y + z = 100 \mid 1 \le x < 4$
5 has 1 factor

$405 \le n < 410$

7) $x' \mapsto 19x + 17 \mod 26$

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

H	E	L	P	Plaintext
7	4	11	15	encrypted
20	15	18	16	enloded
U	P	S	Q	enloded text

UPSQ

7b) U X T D R E N U P S Q F X H
20 23 19 3 17 4 13 20 15 18 16 5 23 7
7 14 22 2 0 13 8 7 4 11 15 24 14 20
H O W C A N I H E L P Y O U

How Can I help you

$11x' + 21 = x \mod 26$

8) $x' \mapsto 11x + \beta \mod 26$

$19(x' - \beta) = x$

$19x' - \beta = x$

Thanks, $\beta = 23$

$P \mapsto 11E + \beta$

$E \mapsto 19P + \alpha \quad \alpha = 5$

$P \mapsto 11E + 23 \quad \beta = 23$

9) JVMMAXCV

WELLDONE

$5E + 3 \mapsto P \mod 26$

$5E + 3 = P$

$5E = P + 23$

$E = 21P + 15$

$\alpha = 21$

$\beta = 15$

10) $2020^{2020} \mod 97$

$2020 \equiv 80 \mod 97$

$80^{2020} \mod 97$

$a^p \equiv a \% p$

$80^{96 \cdot 21 + 4} \mod 97$

$a^{p-1} \equiv 1 \% p$

$(80^{96})^{21} \cdot 80^4 \Rightarrow 1^{21} \cdot 80^4$

$2020^{2020} \mod 97 \equiv 4$

b) $51493^{87494} \mod 5147$

$23^{87494} \mod 5147$

$23^{5146 \cdot 17 + 12} \Rightarrow (23^{5146})^{17} + 23^{12} \mod 5147$

$23^{12} \mod 5147 \equiv 1706 \mod 5147$

10C) $14483426^{1671675} \bmod 1114111$

$11124094^{1671675}$

$11140941^{111410 \cdot 15+5}$

$(1114094^{111410})^{15} + 11140941^{5} \bmod 1114111$

$808365 \bmod 1114111$

11a) $12200^{18162} \bmod 1010$

$12200 \equiv 0 \bmod 2$

$0 \bmod 5$

$80^{100 \cdot 122+0} \bmod 101 = 1 \bmod 101$

$0^{18162} \bmod 2$

$0^{18162} \bmod 5$

$80^{18162} \bmod 101$

$x \equiv 0 \bmod 2$

$\equiv 0 \bmod 5$

$\equiv 1 \bmod 101$

N	b	m	n	x^{-1}	$\pi_b n x$
1010	0	2	505	1	0
	0	5	202	3	0
	1	101	10	91	910
					Σ 910

$910 \bmod 1010$

b) $2000^{4068296} \bmod 8221891049$

$(2000^{2010})^{2024} \cdot 2000^{56}$

$(2000^{2016})^{2018} \cdot 2000^{8}$

$(2000^{2026})^{2008} \cdot 2000^{88}$

$2000^{4\ldots} \bmod 2011$

$2000^{\ldots} \bmod 2017$

$2000^{\ldots} \bmod 2027$

$4634002288 \bmod 8221891049$

12) $600!$ mod 617

$616\ 615\ 614\ 613\ 612\ 611\ 610\ 609\ 608\ 607\ 606\ 605\ 604\ 603\ 602\ 601\ 600!$
$\equiv -1 \bmod 617$

$-1\ -2\ -3\ -4\ -5\ -6\ -7\ -8\ -9\ -10\ -11\ -12\ -13\ -14\ -15\ -16\ 600!$

$(418)16!\ 600! \equiv 1 \bmod 617$

$600! \equiv \boxed{418 \bmod 617}$