Elementary Number Theory

1. $\overline{0} = \overline{104}$, $\overline{3} = \overline{-49}$.
2. $\mathbb{Z}_{22}^* = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21 \bmod 22\}$. The corresponding inverses are $1, 15, 9, 19, 5, 17, 3, 13, 7, 21 \bmod 22$.
3.

```
sage: n=123456789012345;a=5377543210987654321;b=12345678914335
sage: factor(n);factor(a);factor(b)
3 * 5 * 283 * 3851 * 7552031
211 * 15259 * 22541 * 74097269
5 * 13 * 17891 * 10616149
sage: mod(a+b,n); mod(a*b,n); power_mod(a,b,n)
24740866845146
49827615257065
84949384381336
sage: mod(1/a,n)
107345536846486
sage: mod(1/b,n)
ZeroDivisionError: Inverse does not exist.
sage: gcd(a,b)
1
```

The factorization of a and n shows that they have no common factor. Hence a is invertible modulo n. b and n have the common factor 5. Hence b is not invertible modulo n. The factorization shows that a and b are relatively prime. Note that a factorization is not required in order to check whether two numbers are relatively prime; computing the greatest common divisor with the Euclidean Algorithm is sufficient.

4. The Extended Euclidean Algorithm of 1234 and 6789 gives $gcd = 1$, $x = -1700$, $y = 309$.
5. $897 : 32 = 28$, remainder 1. Hence $897 = 28 \cdot 32 + 1$ and $1 = 897 - 28 \cdot 32$. This gives $32^{-1} \equiv -28 \equiv 869 \bmod 897$.
6. $\varphi(2p) = p - 1$, $\varphi(2^m) = 2^{m-1}$, $\varphi(p^m) = (p-1)p^{m-1}$.
7.

```
sage: for n in range(1,2000):
            if (is_pseudoprime(2^n - 1) == True):
                  print n,
2 3 5 7 13 17 19 31 61 89 107 127 521 607 1279
```

8.

```
sage: p=(2^607-1);q=(2^1279-1);n=p*q; phi=(p-1)*(q-1)
sage: for e in range(2,100):
            g=gcd(e,phi)
            if g==1:
                  print e,
5 11 13 17 23 25 29 31 37 41 43 47 53 55 59 61 65 67 71 79
83 85 89 97
```

```
sage: e=5;d=mod(1/e,phi)
sage: m=2^1500+2^500+1
sage: c=power_mod(m,e,n)
sage: m0=power_mod(c,ZZ(d),n)
sage: m==m0
True
```

9.
```
sage: count = 0
sage: for n in range(100000):
            q=2*(ZZ.random_element(2^1023))+1
            if (is_pseudoprime(q)==True):
                  count+=1
      print count
294
```

Each run of this experiment is likely to give another result. The approximate number of primes given by the prime number theorem is

$$2 \cdot \frac{100000}{1024 \ln(2)} \approx 282.$$

10. Fast exponentiation:

$$2^{55} \bmod 61 \equiv 2^{32} \cdot 2^{16} \cdot 2^{4} \cdot 2^{2} \cdot 2^{1} \bmod 61 \equiv 57 \cdot 22 \cdot 16 \cdot 4 \cdot 2 \bmod 61 \equiv 21$$

Square-and-Multiply: SQ, MULT, SQ, SQ, MULT, SQ, MULT, SQ, MULT

$$2^{55} \bmod 61 \equiv ((((2^2 \cdot 2)^2)^2 \cdot 2)^2 \cdot 2)^2 \cdot 2 \bmod 61 \equiv 21$$

5 modular squarings and 4 multiplications are necessary.

11. For size $(n) = \text{size}\,(k) = 2048$, at most 2047 modular squarings and 2047 multiplications are required to compute $a^k \bmod n$.