- <u>1.</u> <u>Definition</u>: a natural number x is a **factor** of the natural number y, iff there is a natural number c, with xc=y.
- <u>2.</u> <u>Definition</u>: a natural number is a **prime number**, iff it has exactly two factors, itself and 1.
- 3. <u>Remark</u>: The number 1 is NOT a prime number. (Why?)
- 4. Here is a list of the first few prime numbers:

| - | | - | _ | | | | | | | | ~ - | | | . – | | | | ~ - | |
|----|---|---|---|------------|----|------------|----|----|----|----|-----|-------|-----|-----|----|----|----|-----|-----|
| .) | 2 | 5 | 7 | 11 | 12 | 17 | 10 | 22 | 20 | 21 | 27 | /11 | /12 | 17 | 52 | 50 | 61 | 67 | 71 |
| 4 | 5 | 5 | ' | T T | 10 | 1 / | 10 | 25 | 25 | 31 | 57 | - T T | 75 | | 55 | 55 | 01 | 07 | / 1 |

5. Divisibility tricks: Divisible by 2 if last digit is even. Divisible by 3 if digits sum to a multiple of3. No trick exists for 7. Trick for 11 is more complicated. Otherwise, you must divide.

<u>6.</u> <u>Theorem</u> (Euclid(): The number of prime numbers is infinite.

Proof: Suppose not. Then let Q = the product of all possible prime numbers. Consider Q+1. Q+1 cannot be divisible by any of the prime numbers, because the remainder when dividing by that prime number would be 1 (not zero). Therefore, either there is another prime not in the list of primes, that is less than Q+1, that is a factor of Q+1; or else Q+1 is itself prime. Either way, the original list of primes was not complete. So there cannot be a finite number of primes.

- 7. <u>Definition</u>: If natural number C is not prime, we say it <u>can be factored</u>.
- <u>8.</u> <u>Remark</u>: suppose AB=C. Suppose $A \le B$. Then, either A < B or A = B.
- <u>9.</u> <u>Theorem</u>: Suppose C is a natural number. If C can be factored, then C has a factor A with A $\leq \sqrt{C}$.

Proof: follows from the remark above.

<u>10. Algorithm</u>: **How to factor a natural number into prime factors**:

If C is a natural number, then we should try to divide C by each prime number less than or equal to the square root of C. If one of those primes is a factor, then C can be factored. Suppose p_1 is that factor. Let $C_1 = C/p_1$. Then continue as before, using C_1 in place of C. Continue until the result is prime. Write the result as a product of primes in ascending order, with exponents.

<u>11. Example</u>: Factor 323 into prime factors.

We need to try the primes 2,3,5,7,11,13,17. Since $18^2 = 324$ (bigger than 323), we don't have to try any primes bigger than 17. After we divide each of these into 323, we find that 17(19)=323. Therefore 323 = 17⁻19.

<u>12. Example</u>: Factor 96 into prime factors. 96/2 = 48. 48/2 = 24. 24/2 = 12. 12/2 = 6. 6/2 = 3. Therefore, 96 = 2^{5.}3.

13. Example: Factor 331 into prime factors.

19² =361 (greater than 329), so we don't need to try any primes bigger than 17. When we try the primes 2,3,5,7,11,13,17, we find that there is a non-zero remainder for each division. Therefore, 331 is a prime number.

<u>14.</u> Exercise: Factor these numbers into prime factors if possible:

12, 28, 64, 100, 132, 327, 441, 1058, 1728.