Session 15 – Prime and Composite Numbers

Computer Security

> *Personal, business, and government information such as social security numbers, bank accounts, credit card numbers, or national security information is transmitted on the Internet daily. It is very important to transmit information concerning individuals, companies, and government securely. This is normally done using Public Key Cryptography. Public Key Cryptography is based on properties of prime numbers.*

Prime Numbers

Prime numbers are a very special type of counting number (natural number). To be a *prime number*, the number must have exactly two distinct counting number (natural number) factors

Example: The value seven, 7, is a prime number because the only counting number factors are 1 and 7. That is, $7 \cdot 1 = 7$ and there is no other pair of counting numbers that when multiplied give a product of 7.

Example: The value six, 6, is not a prime number because 1, 2, 3, and 6 are all counting number factors of six. That is, $1 \cdot 6 = 6$ and $2 \cdot 3 = 6$. Since six has four factors, six cannot be a prime number.

Example: The value one, 1, is not a prime number because the only counting number factor of one is one. That is, $1 \cdot 1 = 1$ is the only product of counting numbers to result in one. Since the definition of a prime number required exactly two distinct counting number factors, one cannot be a prime number.

Note that definition of a prime number excludes the possibility that 1 is a prime. For this reason, many people state that a prime number must be greater than 1 and its only counting number factors are itself and 1.

Definition of Prime and Composite Numbers: We say that a natural number, $p > 1$, is prime if its only natural number factors are p and 1. If a natural number is not prime, then we say that it is *composite*.

Composite Numbers

The above definition implies that any counting number (natural number) that has more than two factors (is greater than 1 and is not prime) is a *composite number*.

Example: The value six, 6, is a composite number because it has four counting number factors: 1, 2, 3, and 6. We have $1 \cdot 6 = 6$ and $2 \cdot 3 = 6$.

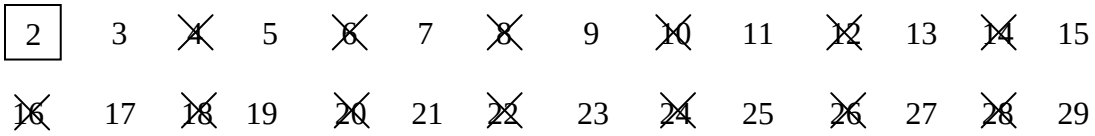
It turns out that mathematicians have declared that 1 is neither prime nor composite. The reason for this has to do with "prime factorization" which is the topic of the next session.

Finding Prime Numbers

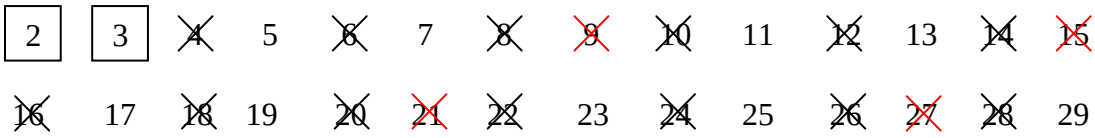
We can find prime numbers using a process called the "Sieve of Eratosthenes". Eratosthenes (276 – 195 BC) was a Greek mathematician who, in addition to developing this process for finding prime numbers, is also credited with being the first to accurately calculate the circumference of the Earth and the distance from the Earth to the sun. He also developed the first map of the world.

Using Eratosthenes' method, we begin by listing every counting number (natural number) greater than 1 up to as big as we want to go. In our example, we will only go up to 29 for now, but a grid for finding all the primes up to 100 is at the end of this lesson.

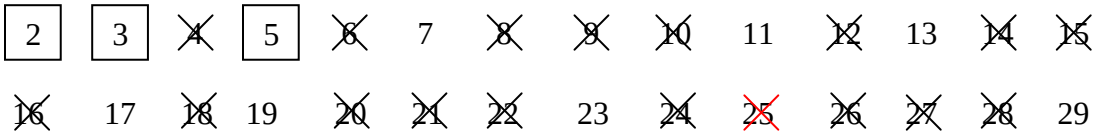
The process is a systematic way of circling values we know are prime and crossing out values we know must be composite. For instance, since the set of the only factors of 2 is {1, 2}, the smallest prime must be 2. We circle it. Then we cross out all the other multiples of 2 because those multiples must be composite. We know they must be composite because, in addition to 1 and themselves, they also have 2 as a factor.



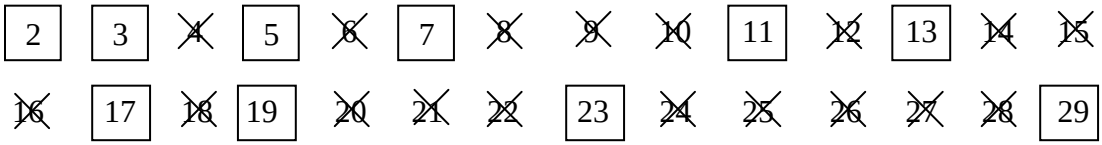
Then we move to the next number in the list that is not already crossed out. It is 3. We know that 3 must be prime because the only number in the list less than 3 is 2, and we have already eliminated all the numbers that have 2 as a factor. (Or, the only counting number factors of 3 are 1 and 3.) So we circle 3 and then cross out all multiples of 3. It is alright that some have already been crossed out such as 6. We just need to be sure that all the multiples of 3 have been eliminated from our list.



Now we circle 5 and cross out all the other multiples of 5 in this list that would be 10, 15, 20, and 25, all but 20 are already crossed out.



We circle the 7 and cross out all the multiples of 7. The only other multiples of 7 in the list are 14, 21, and 28 all of which are already crossed out. We circle 11. The only other multiple of 11 on the list is 22 which is already crossed out. We circle 13 and the multiple 26 is already crossed out. In a longer list of numbers, there could be multiples we would need to cross out. The only numbers remaining are 17, 19, 23, and 29, and they have no other multiples in the list either. We circle them.



We now have a list of all the prime numbers that are between 1 and 30. The set of primes between 1 and 30 is {2, 3, 5, 7, 11, 13, 17, 19, 23, 29}.

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100