Lecture 4: Worksheets

The Ulam Spiral

Fill in the primes into the Ulam spiral.

197	196	195	194	193	192	191	190	189	188	187	186	185	184	183	240
198	145	144	143	142	141	140	139	138	137	136	135	134	133	182	239
199	146	101	100	99	98	97	96	95	94	93	92	91	132	181	238
200	147	102	65	64	63	62	61	60	59	58	57	90	131	180	237
201	148	103	66	37	36	35	34	33	32	31	56	89	130	179	236
202	149	104	67	38	17	16	15	14	13	30	55	88	129	178	235
203	150	105	68	39	18	5	4	3	12	29	54	87	128	177	234
204	151	106	69	40	19	6	1	2	11	28	53	86	127	176	233
205	152	107	70	41	20	7	8	9	10	27	52	85	126	175	232
206	153	108	71	42	21	22	23	24	25	26	51	84	125	174	231
207	154	109	72	43	44	45	46	47	48	49	50	83	124	173	230
208	155	110	73	74	75	76	77	78	79	80	81	82	123	172	229
209	156	111	112	113	114	115	116	117	118	119	120	121	122	171	228
210	157	158	159	160	161	162	163	164	165	166	167	168	169	170	227
211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226

Infinitely many primes

Euclid's proof starts with the assumption that there are only finitely many primes. Enumerate them $p_1, ..., p_k$. We can now form the number $n = p_1 p_2 \cdots p_k + 1$. This number is not divisible by any of the primes because it leaves rest 1. Since the number n can not be divisible by any prime, it must be a prime itself, but larger than any p_j. This contradicts that the list of primes was complete.

2. Arbitrary large gaps of primes

For every n, there exist consecutive primes which differ by at least n.

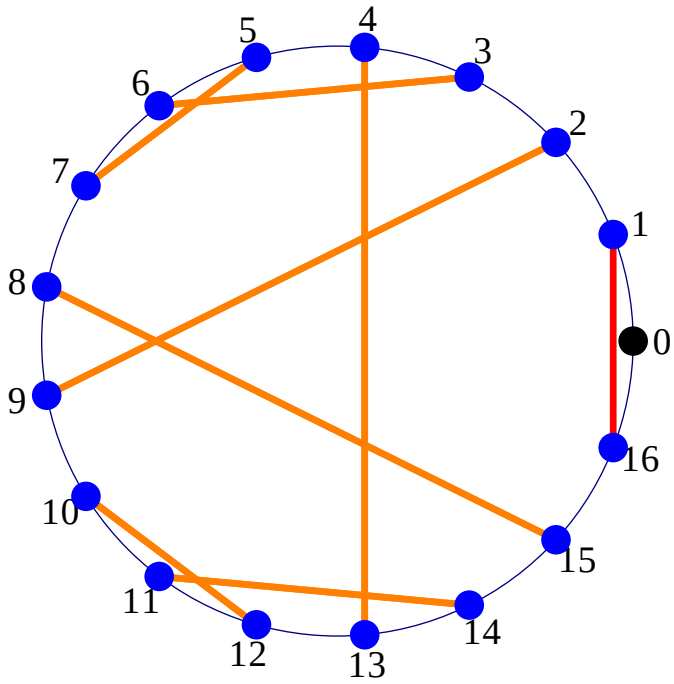
Show that all integers $n! + 2, \ldots, n! + n$ are composite.

2. Wilson's theorem

n is a prime if and only if $(n-1)! + 1$ is divisible by n.

The proof of the theorem has two directions:

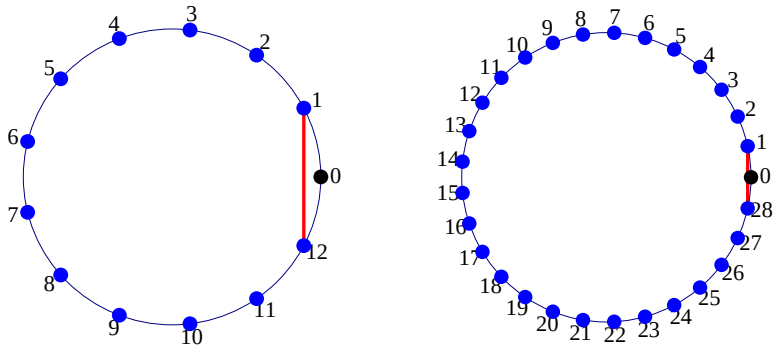
If n is a prime, then the equation $xy = 1 \bmod n$ with different x, y has exactly one pair of solution. For $x^2 = 1$, there is only the solution $1, -1$.



Wilson's theorem in the case $p = 17$. We find all pairs which multiply to 1 Like $2 * 9 = 18, 3 * 6 = 18, 4 * 13 = 52, 8 * 15 = 120$ which all leave rest 1 when dividing by 17. Only the numbers 1 and -1 do not pair. The product $(n-1)!$ multiplies all the numbers together and gives

$(-1) \cdot 1(2*9)(3*6)(4*13)(5*7)(8*15)(10*12)(11*14) = -1$.

Problem 1) Verify the proof either in the case $p = 13$ or $p = 29$.



If $n = pq$ is not a prime and larger than 4, then $(n-1)!$ is divisible by n because it is a multiple of p and q.

Problem 2) Verify this in the concrete case of $n = 15$. Why is

$$15! = 1*2*3*4*5*6*7*8*9*10*11*12*13*14$$

a multiple of 15?

Fermat's little theorem

We look at the proof of Fermat's theorem which states that

$a^p - a$ is divisible by p for all prime p.

The **binomial formula** is

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + ... + \binom{n}{n-1} ab^{n-1} + b^n$$

In the case $b = 1$ it means

$$(a+1)^n = a^n + \binom{n}{1} a^{n-1} + \binom{n}{2} a^{n-2} + ... + \binom{n}{n-1} a + 1$$

4. The steps

1. Check that Fermat's theorem is true for $a = 0$ and $a = 1$.

2. Verify that the induction step from a to $a+1$ is equivalent to show that

$$(a+1)^p - a^p - 1$$

is divisible by p if p is a prime.

3. Verify that $(a+1)^p - a^p - 1$ is divisible by p if all all binomial coefficients

$$\binom{p}{m} = \frac{p!}{m!(p-m)!} = \frac{p \cdot (p-1)... \cdot (p-m+1)}{m \cdot (m-1) \cdot ... \cdot 1}$$

are divisible by p.

4. Verify that $\frac{p \cdot (p-1)... \cdot (p-m+1)}{m \cdot (m-1) \cdot ... \cdot 1}$ divisible by p if p is prime.

This is illustrated by the **Pascal triangle**. For rows which are prime, the interior entries are all divisible by the row number. For example, for $p = 5$, the middle entries $5, 10, 10, 5$ are all divisible by 5.