Miller-Rabin Primality Test

Gary Fredericks

September 22, 2014

About Me

- Software engineer at Groupon
- Fan of pure math, theoretical CS
- `@gfredericks_`

Why Number Theory?

About This Paper

- "Probabilistic Algorithm for Testing Primality"
- Michael O. Rabin, 1977
- Modifies a deterministic but presumptive algorithm published by Gary L. Miller in 1976
- The algorithm has become known as the "Miller-Rabin Primality Test"
- The paper itself is not very accessible (whoopsie-doodle)

About This Talk

- Motivate the problem
  - I.e., why I like numbers
- Describe the algorithm
- Try to give an intuition for why it works

Numbers

Numbers

$0, 1, 2, 3, 4, 5, 6, \ldots$

$3 + 8 = 11$

$6 \cdot 7 = 42$

Addition

Addition shifts the number line.

```
0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,16,...
+ 7:                    0, 1, 2, 3, 4, 5, 6, 7, 8, 9,...
```

$? + ? = 53671$

- $0 + 53671$
- $1 + 53670$
- $2 + 53669$
- $3 + 53668$
- $\ldots$
- $53671 + 0$

Multiplication

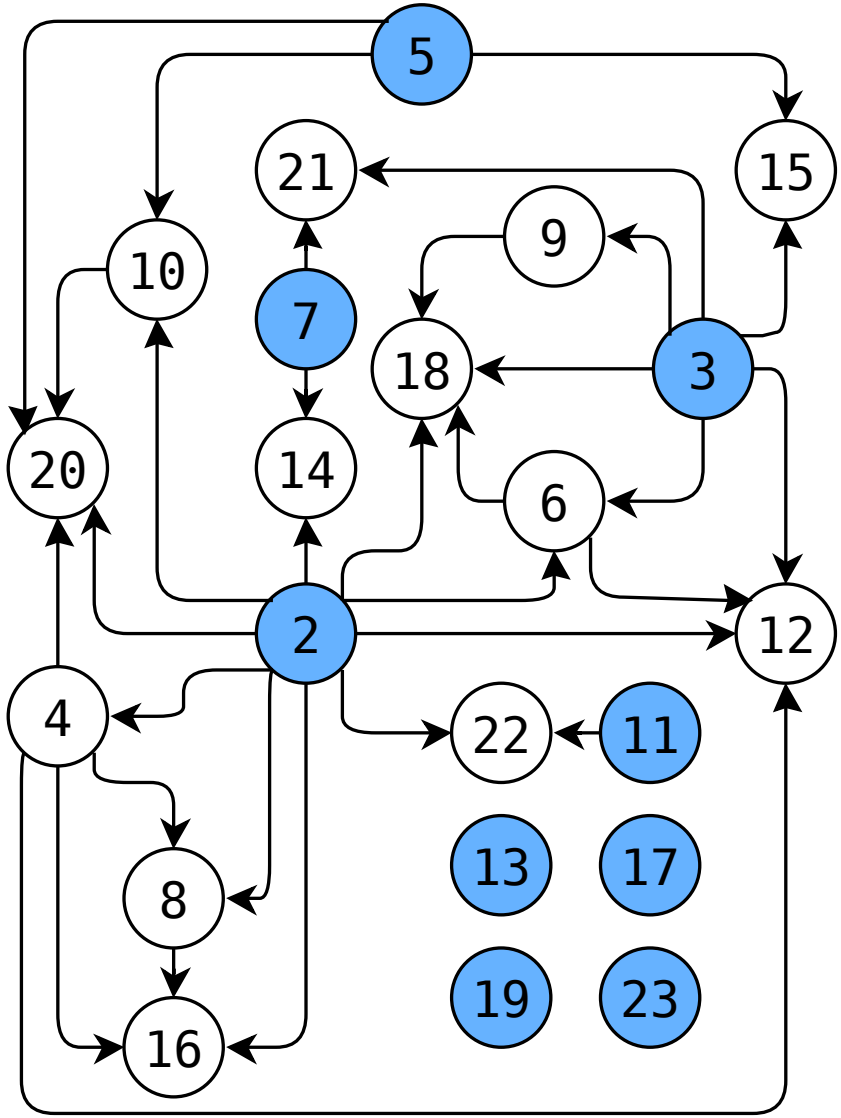
Multiplication scales the number line.

```
1       0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,
2   * 3: 0,       1,       2,       3,       4,       5,
```

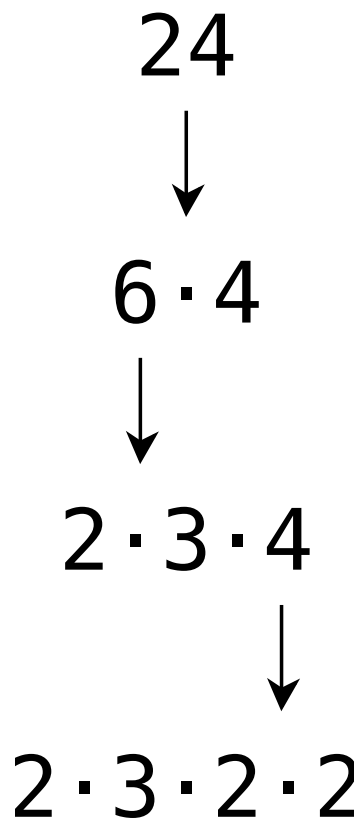
$? \cdot ? = 53671$

- $1 \cdot 53671$
- $53671 \cdot 1$
- Um...

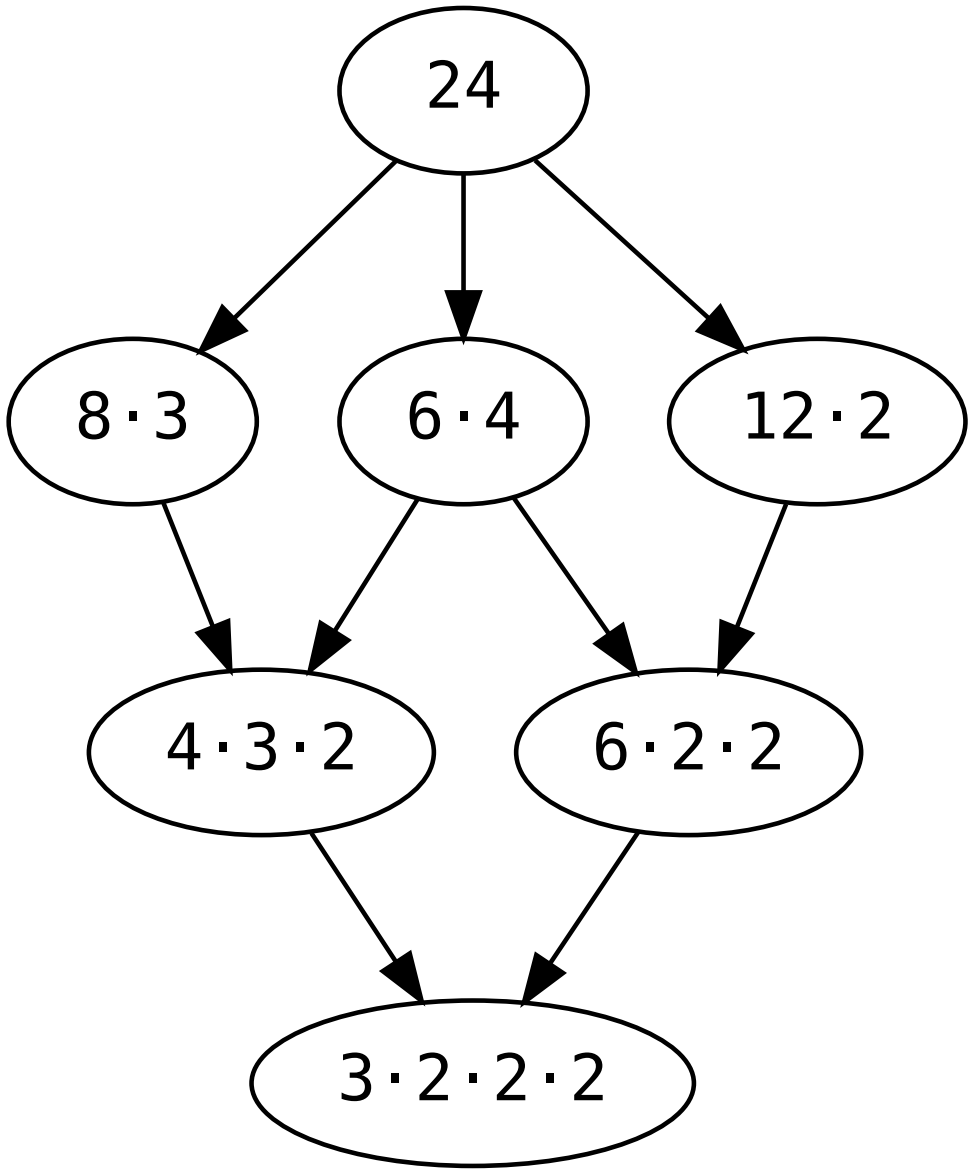
Divisibility Graph



Factoring 24

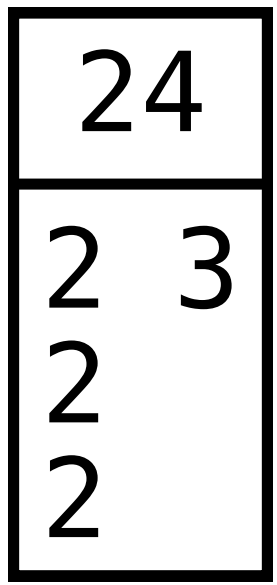


Unique Factorizations



Unique Factorizations

A positive integer can be viewed as a multiset of primes.



Unique Factorizations

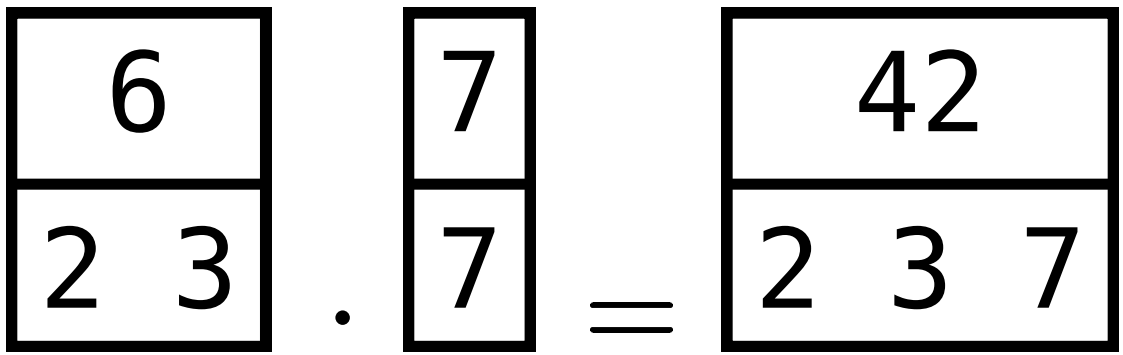
- $1 =$
- $2 = 2$
- $3 = 3$
- $4 = 2 \cdot 2$
- $5 = 5$
- $6 = 2 \cdot 3$
- $7 = 7$
- $8 = 2 \cdot 2 \cdot 2$
- $9 = 3 \cdot 3$
- $10 = 2 \cdot 5$
- $11 = 11$
- $12 = 2 \cdot 2 \cdot 3$
- $13 = 13$
- $14 = 2 \cdot 7$
- $15 = 3 \cdot 5$
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$
- $17 = 17$
- $18 = 2 \cdot 3 \cdot 3$
- $19 = 19$
- $20 = 2 \cdot 2 \cdot 5$
- $21 = 3 \cdot 7$
- $22 = 2 \cdot 11$
- $23 = 23$
- $24 = 2 \cdot 2 \cdot 2 \cdot 3$
- $25 = 5 \cdot 5$
- $26 = 2 \cdot 13$
- $27 = 3 \cdot 3 \cdot 3$
- $28 = 2 \cdot 2 \cdot 7$
- $29 = 29$
- $30 = 2 \cdot 3 \cdot 5$
- $31 = 31$
- $32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$
- $33 = 3 \cdot 11$
- $34 = 2 \cdot 17$
- $35 = 5 \cdot 7$
- $36 = 2 \cdot 2 \cdot 3 \cdot 3$

Concepts explained using unique factorization

- Multiplication
- Division
- Divisibility
- Prime / Composite
- GCD
- Coprimality
- Reduc{ing,ed} fractions
- Which fractions have finite decimal representations
- Which numbers have "obvious" divisors?

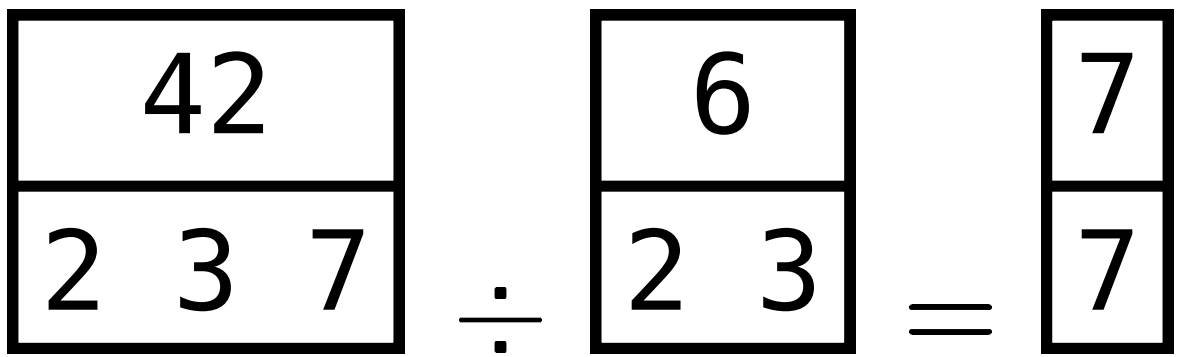
Multiplication

Multiplication is just a multiset sum.



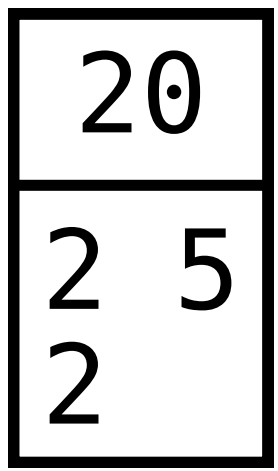
Division

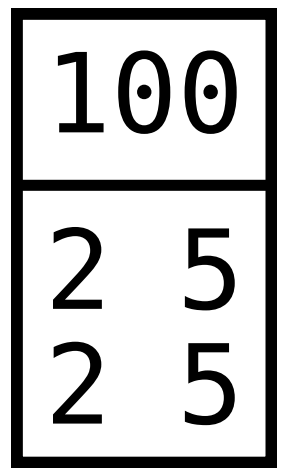
Division is just a multiset difference.



Divisibility

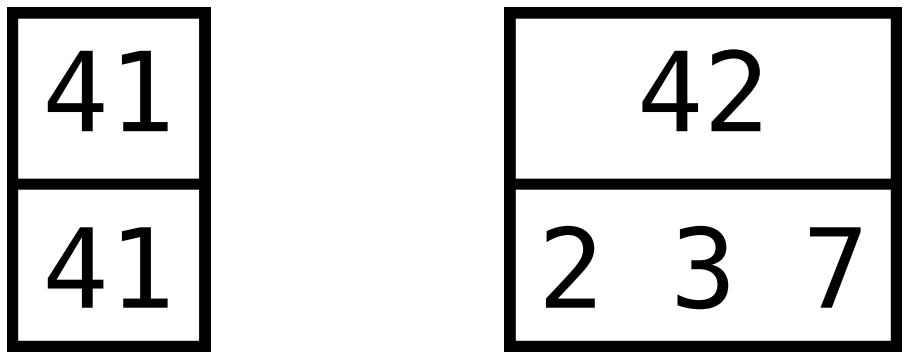
a is divisible by b if b's factorization is a subset of a's.





Prime / Composite

A prime number is a number whose prime factorization is itself.



GCD: 90 and 525

The greatest common divisor (GCD) of two numbers is the intersection of their factorizations.

$$\gcd\left(\begin{array}{|c|}\hline 90 \\ \hline 2\ \ 3\ \ 5 \\ \quad\ 3 \\ \hline\end{array}, \begin{array}{|c|}\hline 525 \\ \hline 3\ \ 5\ \ 7 \\ \quad\ 5 \\ \hline\end{array}\right) = \begin{array}{|c|}\hline 15 \\ \hline 3\ \ 5 \\ \hline\end{array}$$

GCD: 90 and 527

$$\gcd\left(\begin{array}{|c|}\hline 90 \\ \hline 2\ \ 3\ \ 5 \\ \ \ \ 3 \\ \hline \end{array}, \begin{array}{|c|}\hline 527 \\ \hline 17\ \ 31 \\ \hline \end{array}\right) = \begin{array}{|c|}\hline 1 \\ \hline \\ \hline \end{array}$$

Coprimality

Two integers are coprime if they have no factors in common.

90
2 3 5 3

527
17 31

Reduc{ing,ed} fractions

Reducing a fraction just means removing the common parts of the numerator and denominator's factorizations.

$$\frac{90}{525} = \frac{2 \cdot 3 \cdot \cancel{3} \cdot \cancel{5}}{\cancel{3} \cdot \cancel{5} \cdot 5 \cdot 7} = \frac{2 \cdot 3}{5 \cdot 7} = \frac{6}{35}$$

A reduced fraction has a numerator and denominator that are coprime.

Which fractions have finite decimal representations?

- $\frac{1}{2} = 0.5$
- $\frac{2}{3} = 0.\overline{3}\ldots$
- $\frac{3}{4} = 0.75$
- $\frac{4}{5} = 0.8$
- $\frac{5}{6} = 0.8\overline{3}\ldots$
- $\frac{6}{7} = 0.\overline{857142}\ldots$
- $\frac{7}{8} = 0.875$
- $\frac{8}{9} = 0.\overline{8}\ldots$
- $\frac{9}{10} = 0.9$
- $\frac{10}{11} = 0.\overline{90}\ldots$
- $\frac{11}{12} = 0.91\overline{6}\ldots$

Which fractions have finite decimal representations?

- $\frac{1}{2} = \frac{1}{2} = 0.5$
- $\frac{2}{3} = \frac{2}{3} = 0.\overline{3}\ldots$
- $\frac{3}{4} = \frac{3}{2 \cdot 2} = 0.75$
- $\frac{4}{5} = \frac{2 \cdot 2}{5} = 0.8$
- $\frac{5}{6} = \frac{5}{2 \cdot 3} = 0.8\overline{3}\ldots$
- $\frac{6}{7} = \frac{2 \cdot 3}{7} = 0.\overline{857142}\ldots$
- $\frac{7}{8} = \frac{7}{2 \cdot 2 \cdot 2} = 0.875$
- $\frac{8}{9} = \frac{2 \cdot 2 \cdot 2}{3 \cdot 3 \cdot 3} = 0.\overline{8}\ldots$
- $\frac{9}{10} = \frac{3 \cdot 3 \cdot 3}{2 \cdot 5} = 0.9$
- $\frac{10}{11} = \frac{2 \cdot 5}{11} = 0.\overline{90}\ldots$
- $\frac{11}{12} = \frac{11}{2 \cdot 2 \cdot 3} = 0.91\overline{6}\ldots$

Which numbers have "obvious" divisors?

- 1225285014
- 1222105395
- 6431163840
- 2202551775
- 7118220000
- 2729925887

Computational Problems

Factorization Problem

3289540009901
?

Primality testing

Factorization seems to be difficult. [1]

Could it be an easier problem to simply identify whether a number is prime or composite without necessarily determining its factorization? [2]

[1] Without a quantum computer

[2] Yes. Yes of course it could that's what this talk is about.

The Miller-Rabin Primality Test

The Miller-Rabin Primality Test

```
1  (defn probably-prime?
2    "Returns true if n is probably prime,
3    false if it is certainly not. A
4    higher test-count gives exponentially
5    higher certainty when it returns true,
6    but increases the runtime."
7    [n test-count]
8    (let [potential-witness #(+ 2 (rand-int (- n 3)))]
9      (->> (repeatedly test-count potential-witness)
10          (not-any? (fn [b] (witness? n b))))))
```

Probably

The central theorem in the paper is that for any composite number n, at least $\frac{3}{4}$ of the potential witnesses are actually witnesses.

Reality	Asserts prime	Asserts composite
prime	100%	0%
composite	25%	75%

Is it really a prime?

Probability of failure is: $\frac{1}{4^x}$

- 1 run: $\frac{1}{4}$
- 2 runs: $\frac{1}{16}$
- 10 runs: $\frac{1}{1048576}$
- 100 runs:

$$\frac{1}{1606938044258990275541962092341162602522202993782792835301376}$$

What is a witness?

```
1  (defn witness?
2    "Returns true if b is a witness
3    to the compositeness of n."
4    [n b]
5    (or (witness-a? n b)
6        (witness-b? n b)))
```

Where are we headed?

For each of `witness-a?` and `witness-b?`:

- What is the code/logic?
- Why does this correctly detect compositeness?
- How common are the witnesses?

```
witness-a?
```

witness-a?

```
1  (defn witness-a?
2    "Returns true if b^(n-1) is not
3    congruent to 1 mod n."
4    [n b]
5    (not= 1 (pow-mod b (dec n) n)))
```

For primes

```
1  (defn witness-a-density
2    "Returns the fraction of candidate
3    witnesses that meet criteria (a)."
4    [n]
5    (let [c (->> (range 2 n)
6                 (filter (fn [b] (witness-a? n b)))
7                 (count))]
8      (/ c (- n 2))))
9
10 (->> (range 3 10000)
11      (filter prime?)
12      (map witness-a-density)
13      (frequencies))
```

```
;;=> {0 1228}
```

For composites

```
1  (->> (range 10000)
2       (filter composite?)
3       (map witness-a-density)
4       (stats))
```

```
;; Of 8769 numbers...
;; min:    0.20
;; max:    1.00
;; median: 1.00
;; avg:    0.99
;;=> nil
```

witness-a?

```clojure
(defn witness-a?
  "Returns true if b^(n-1) is not
  congruent to 1 mod n."
  [n b]
  (not= 1 (pow-mod b (dec n) n)))
```

Fermat's Little Theorem

For a prime p and $0 < b < p$:

$$b^{p-1} \equiv 1 \mod p$$

Modular Arithmetic

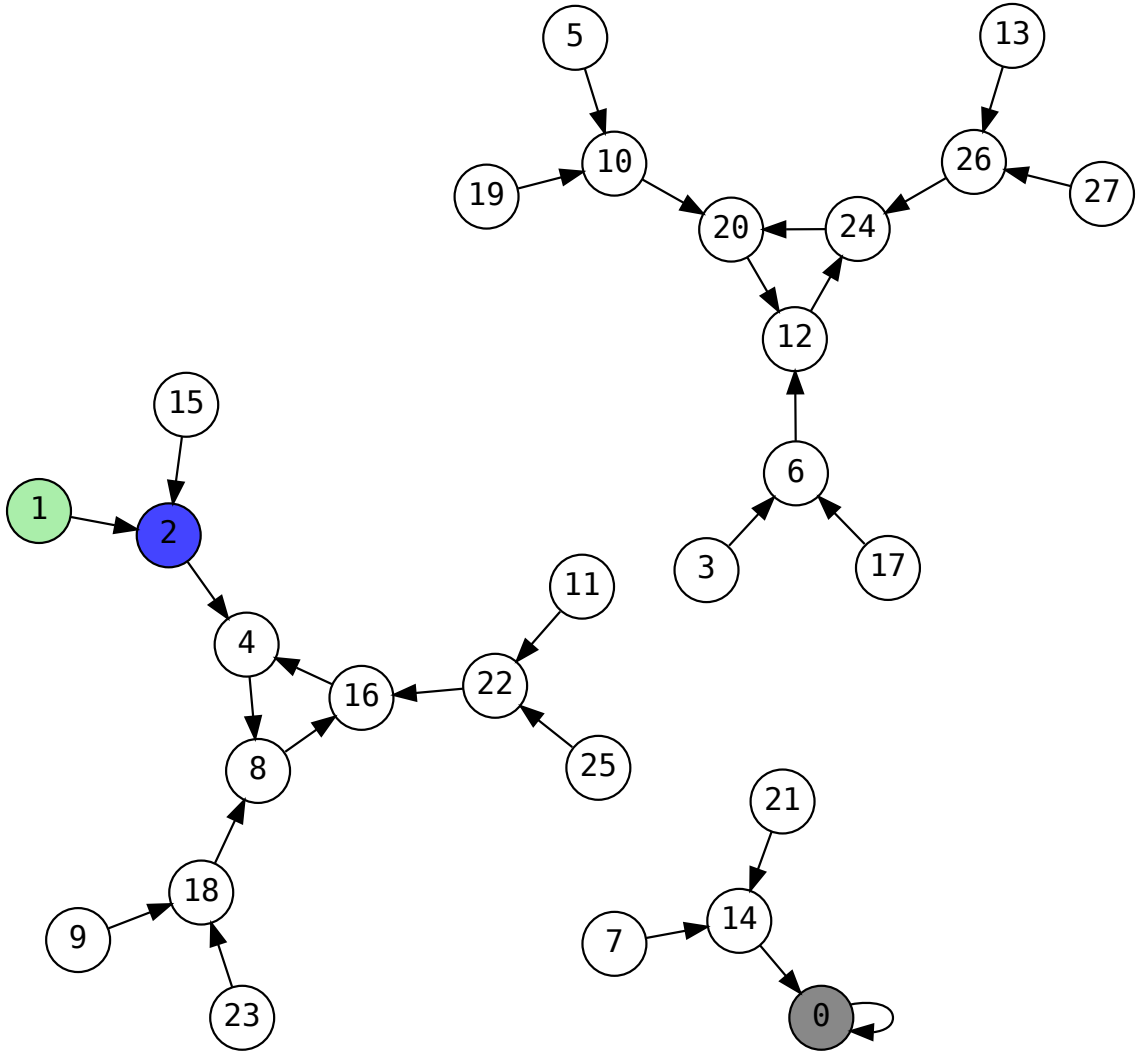
Arithmetic using the integers $0 \ldots n-1$, doing all addition and multiplication $\mod n$.

Multiplication mod 10

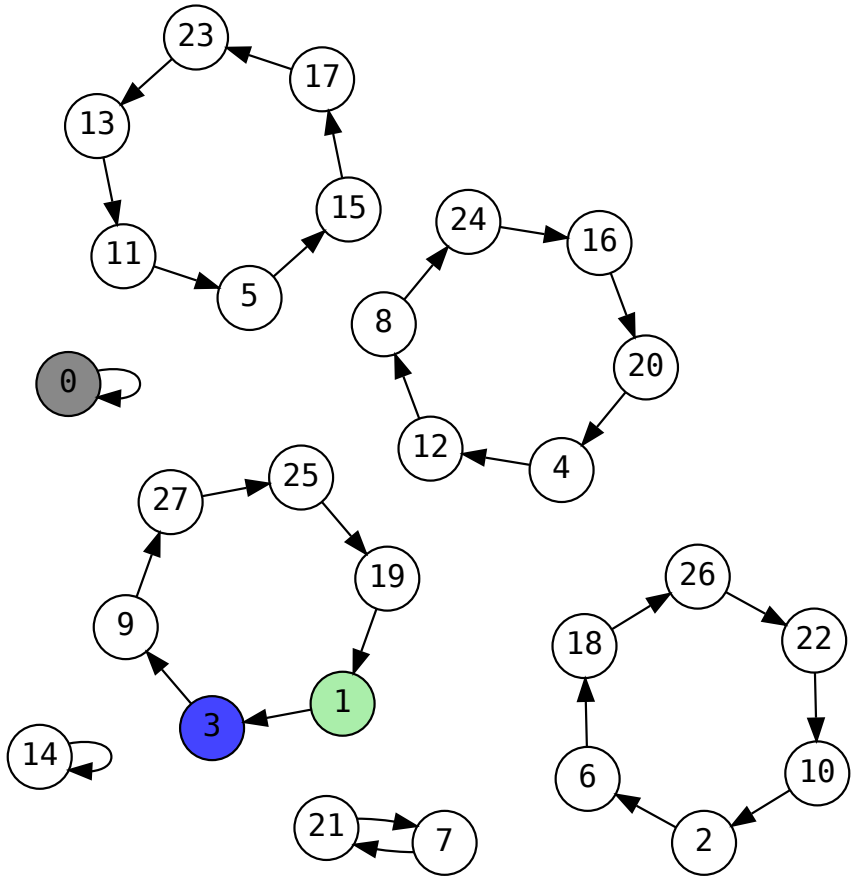
	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Multiplication, $n = 28$

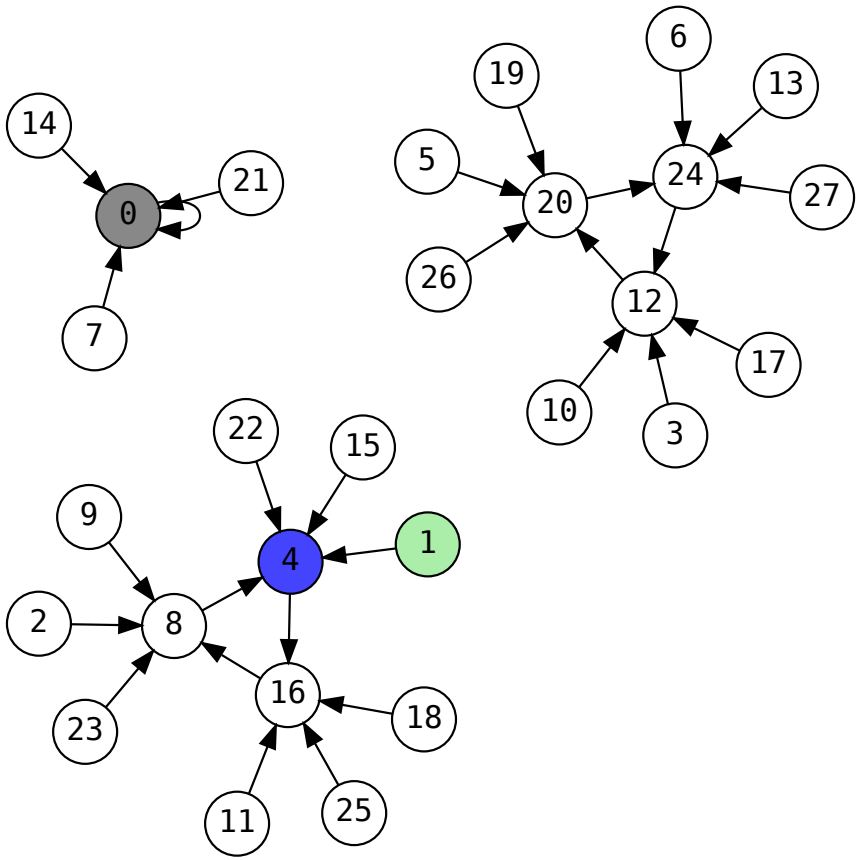
Multiplication, $n = 28, b = 2$



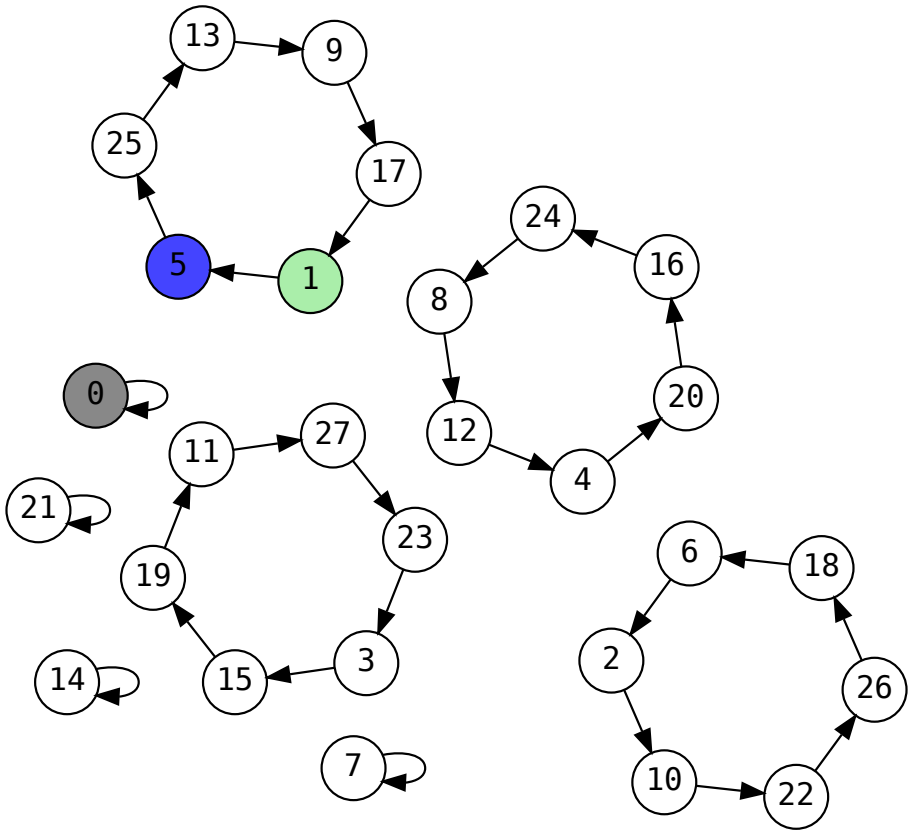
Multiplication, $n = 28, b = 3$



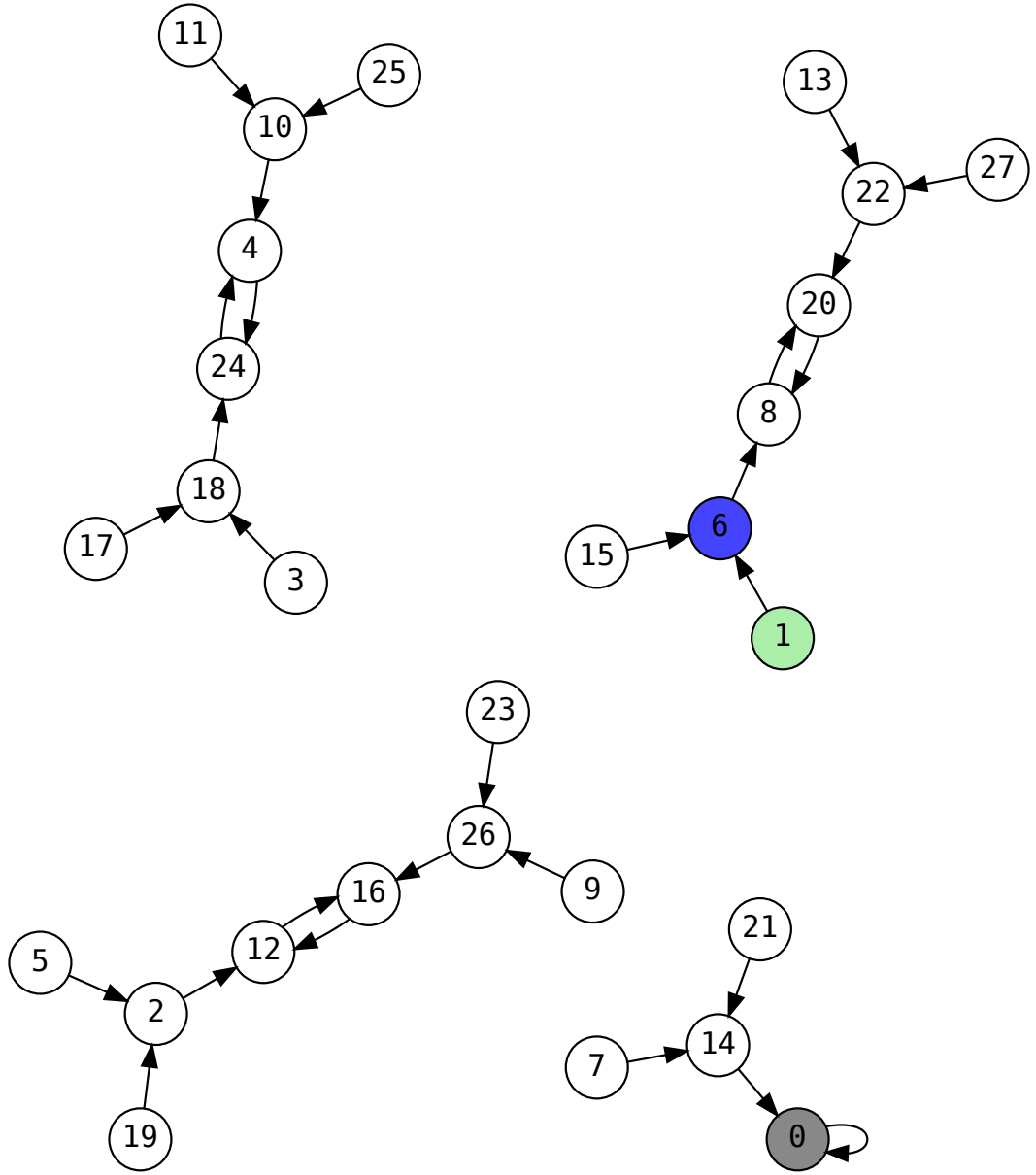
Multiplication, $n = 28, b = 4$



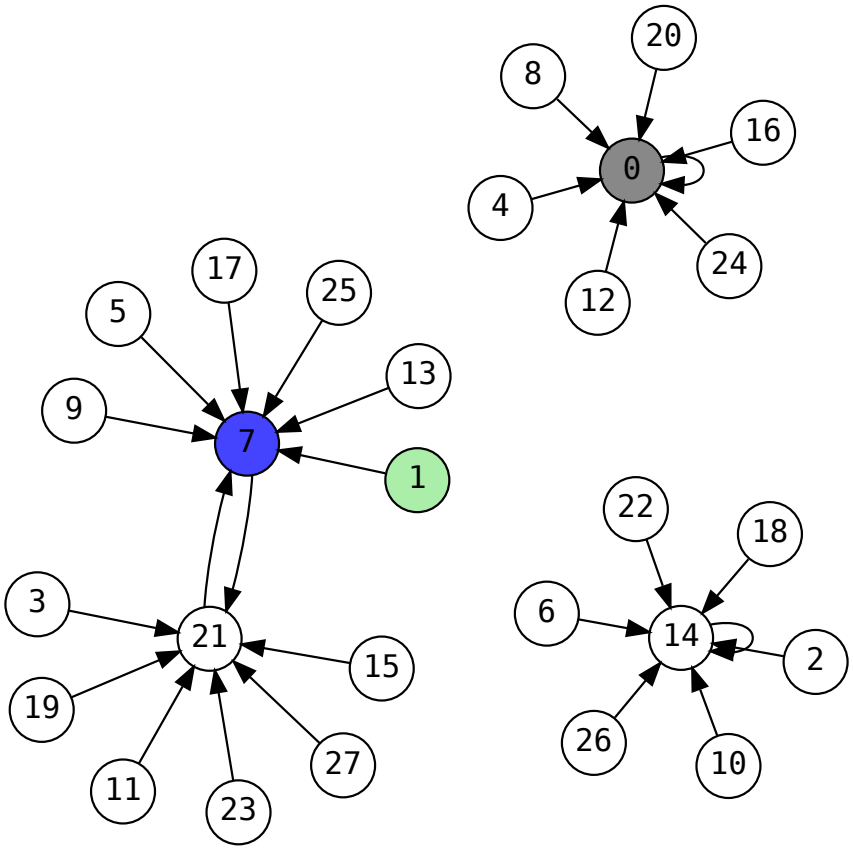
Multiplication, $n = 28, b = 5$



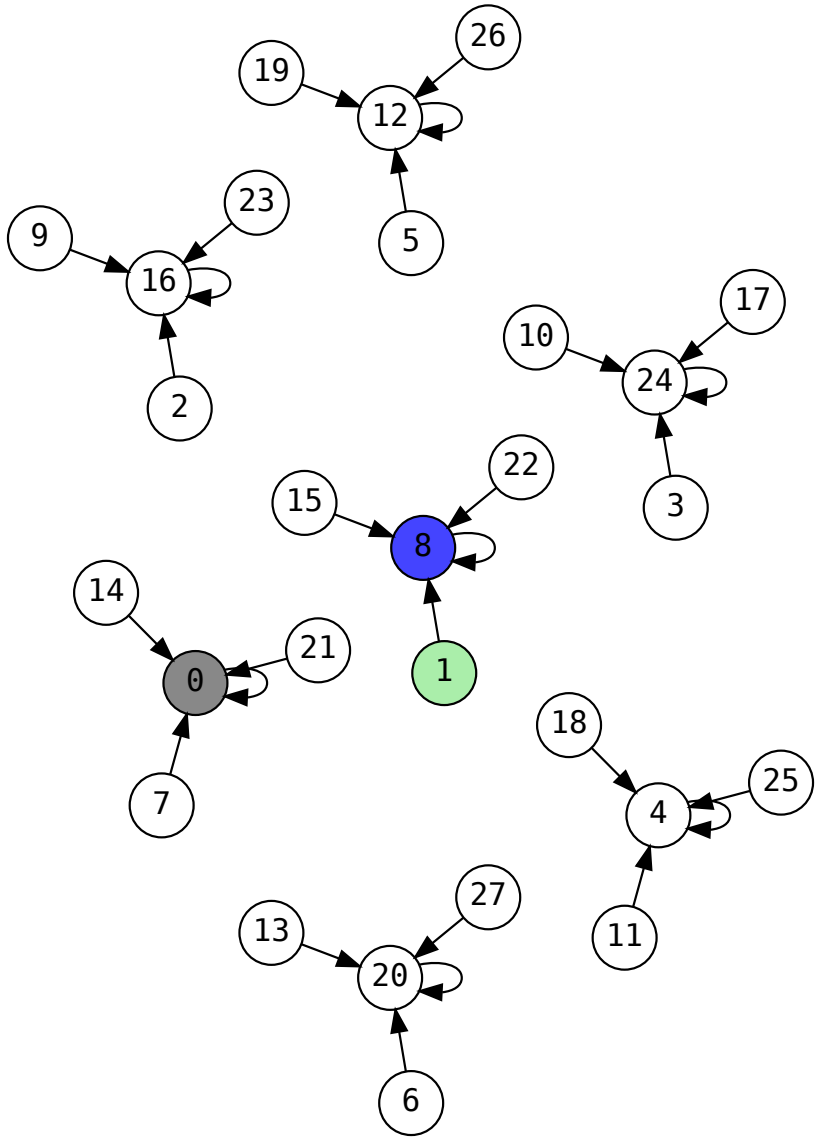
Multiplication, $n = 28, b = 6$



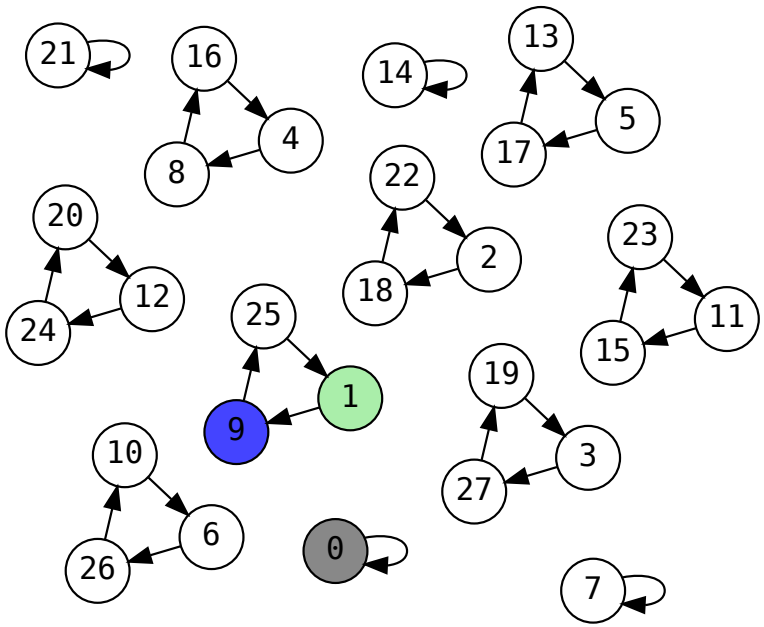
Multiplication, $n = 28, b = 7$



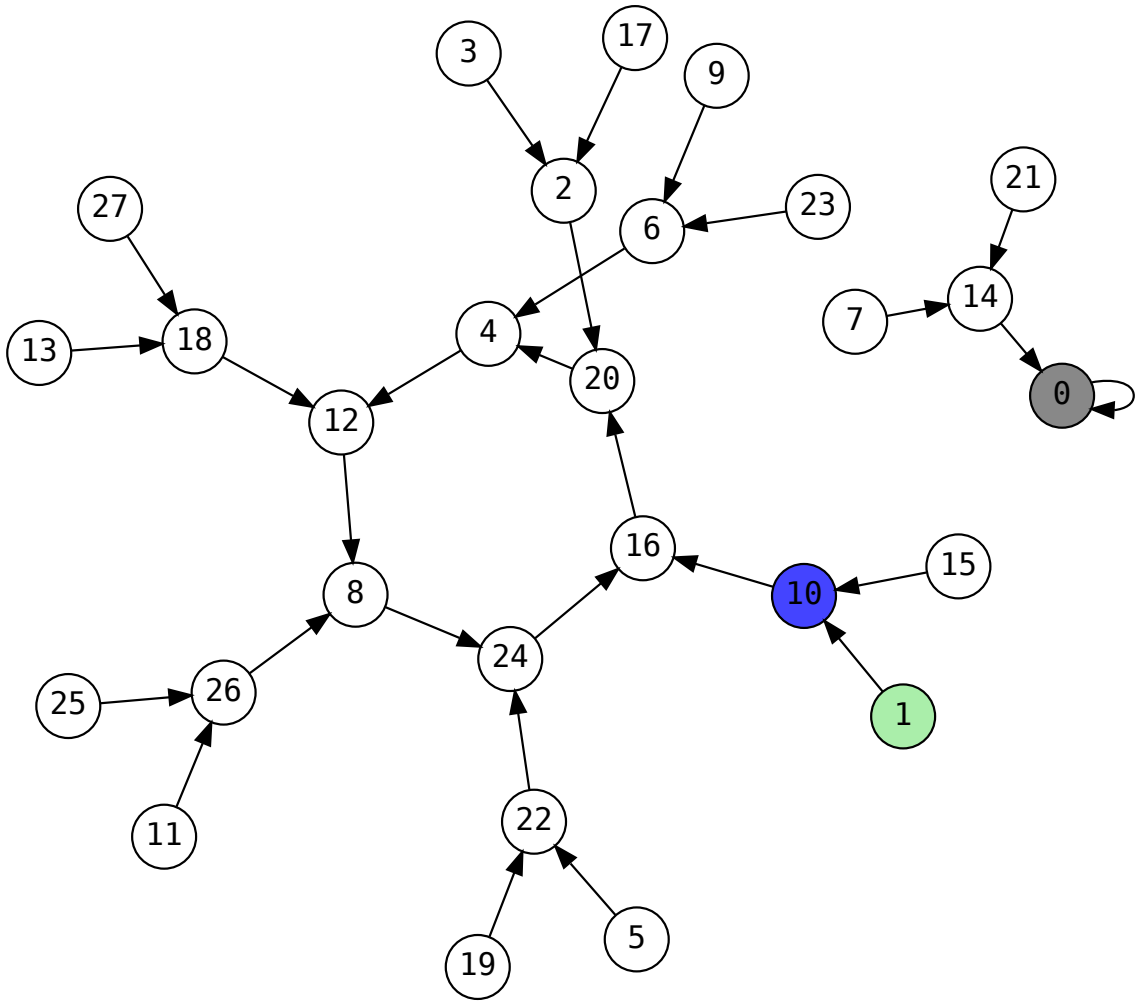
Multiplication, $n = 28, b = 8$



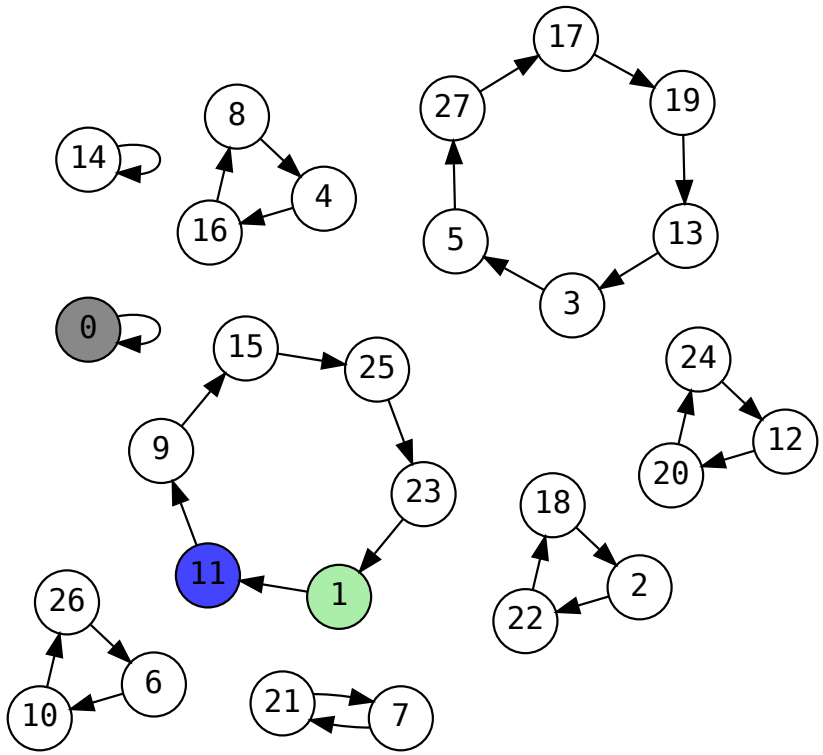
Multiplication, $n = 28, b = 9$



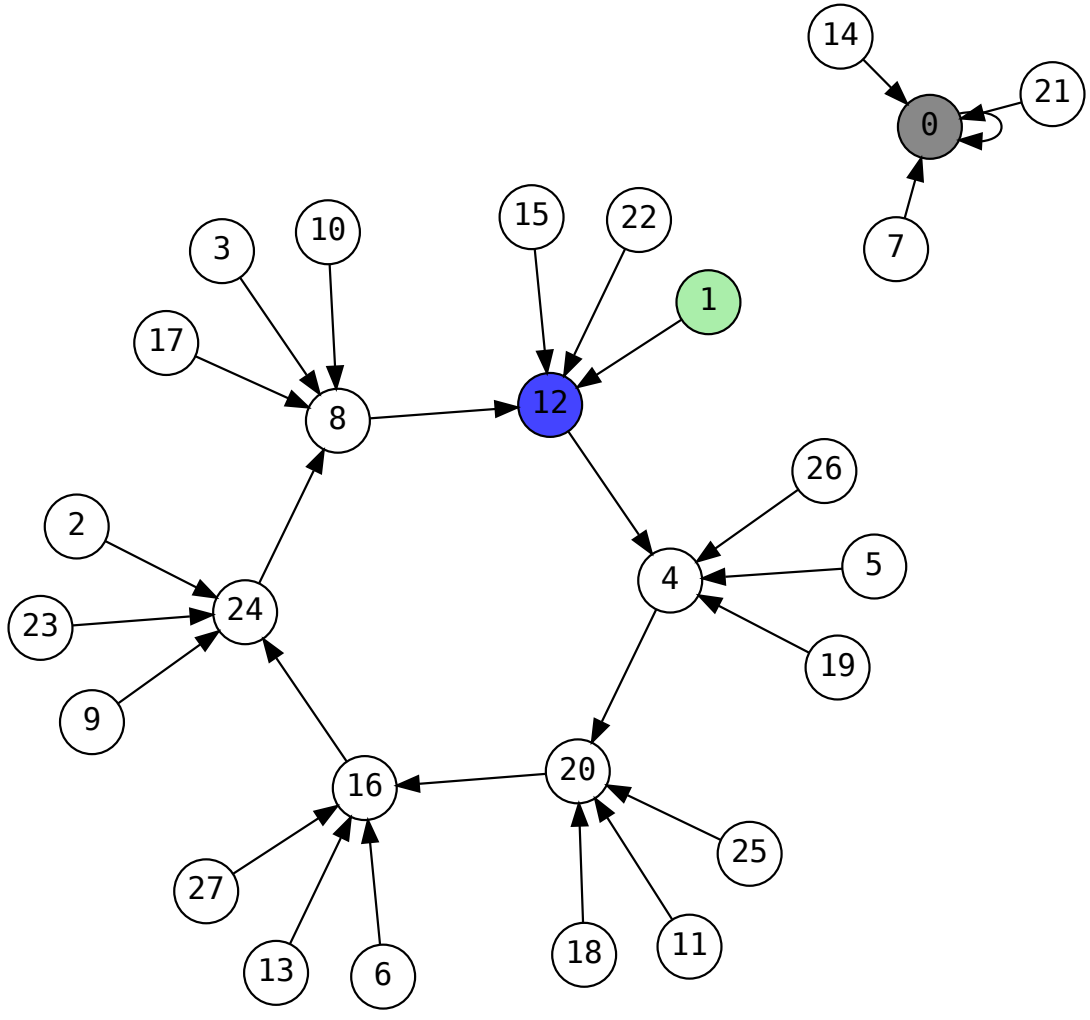
Multiplication, $n = 28, b = 10$



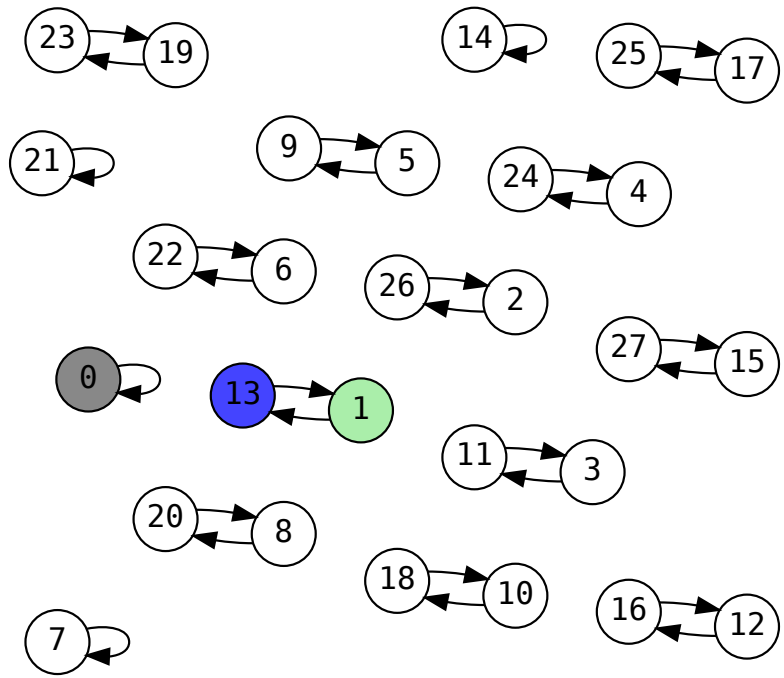
Multiplication, $n = 28, b = 11$



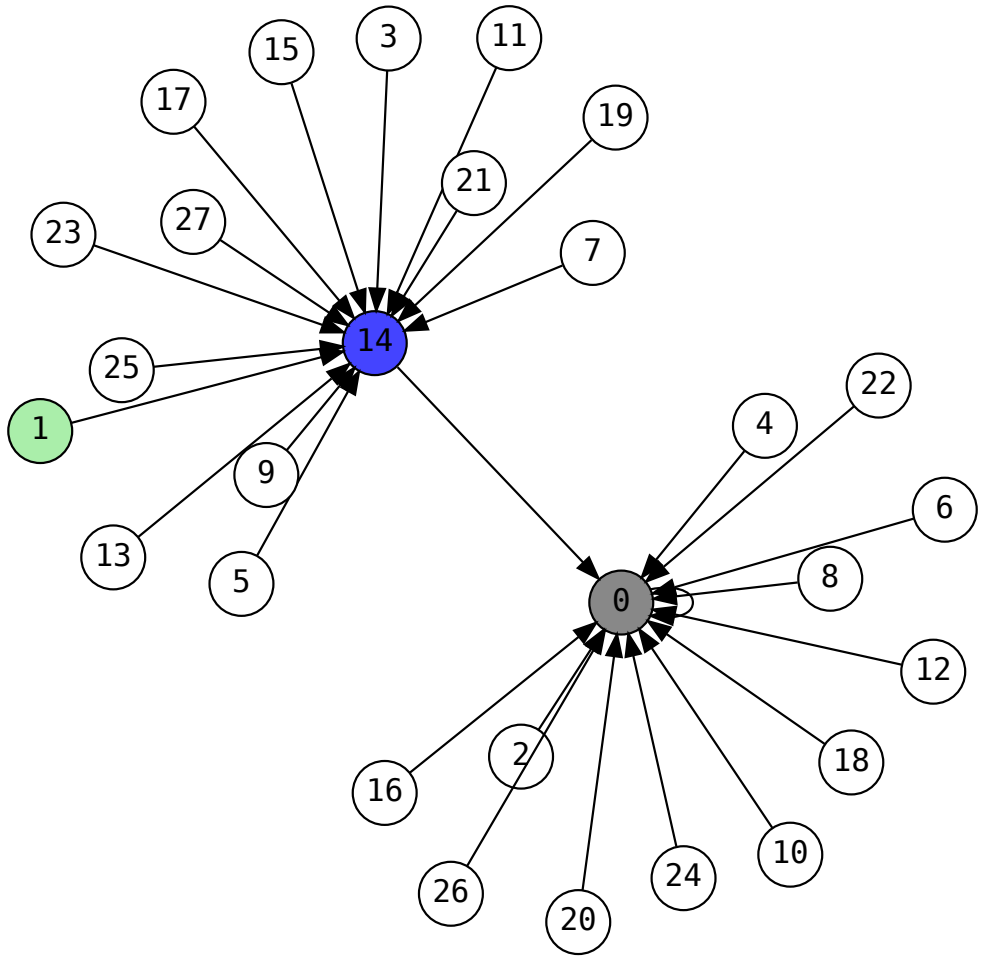
Multiplication, $n = 28, b = 12$



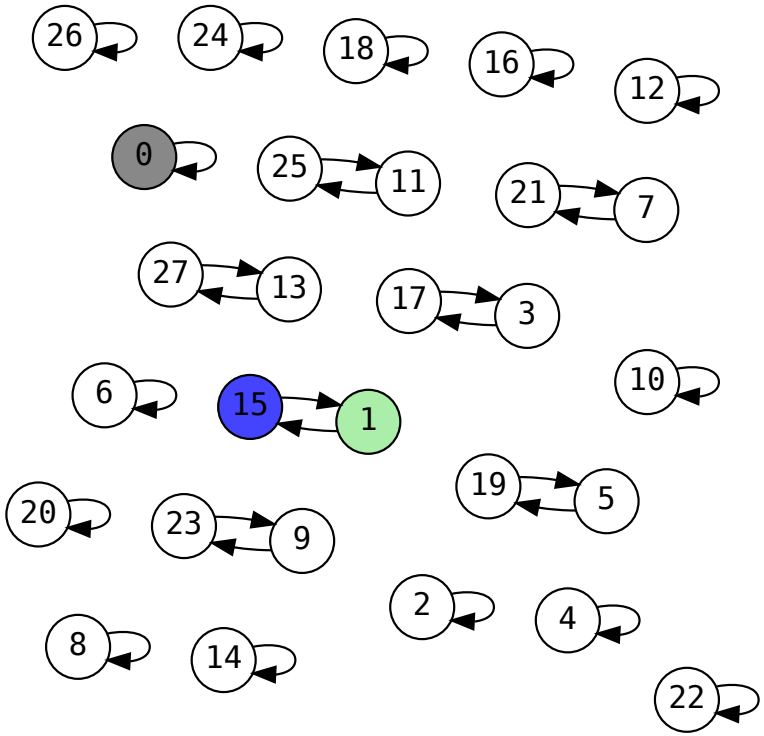
Multiplication, $n = 28, b = 13$



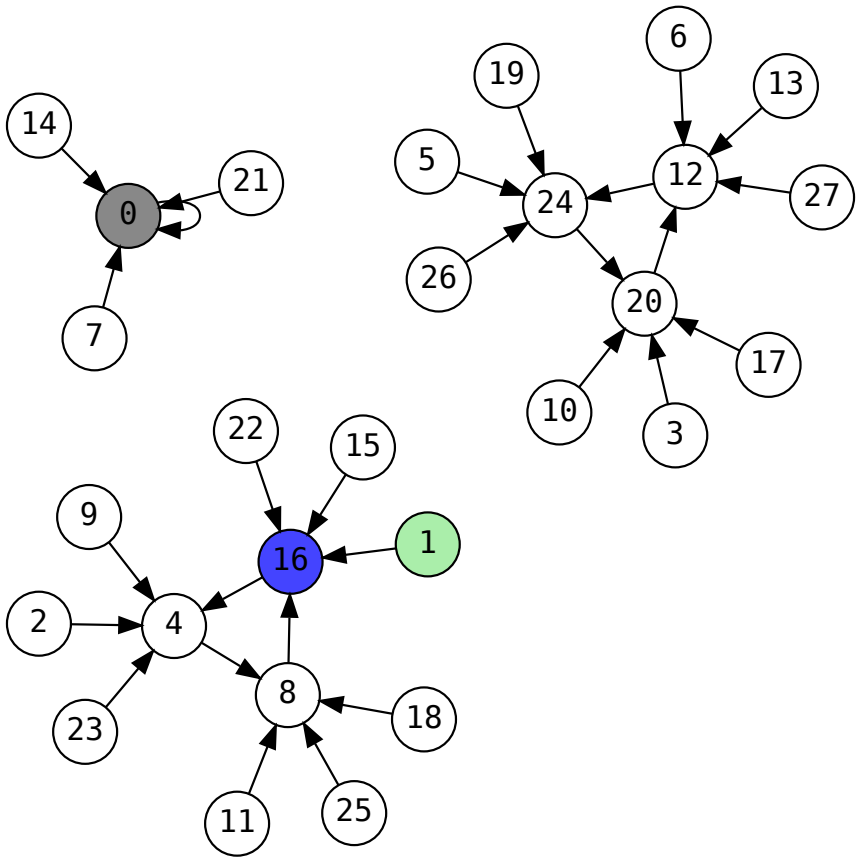
Multiplication, $n = 28, b = 14$



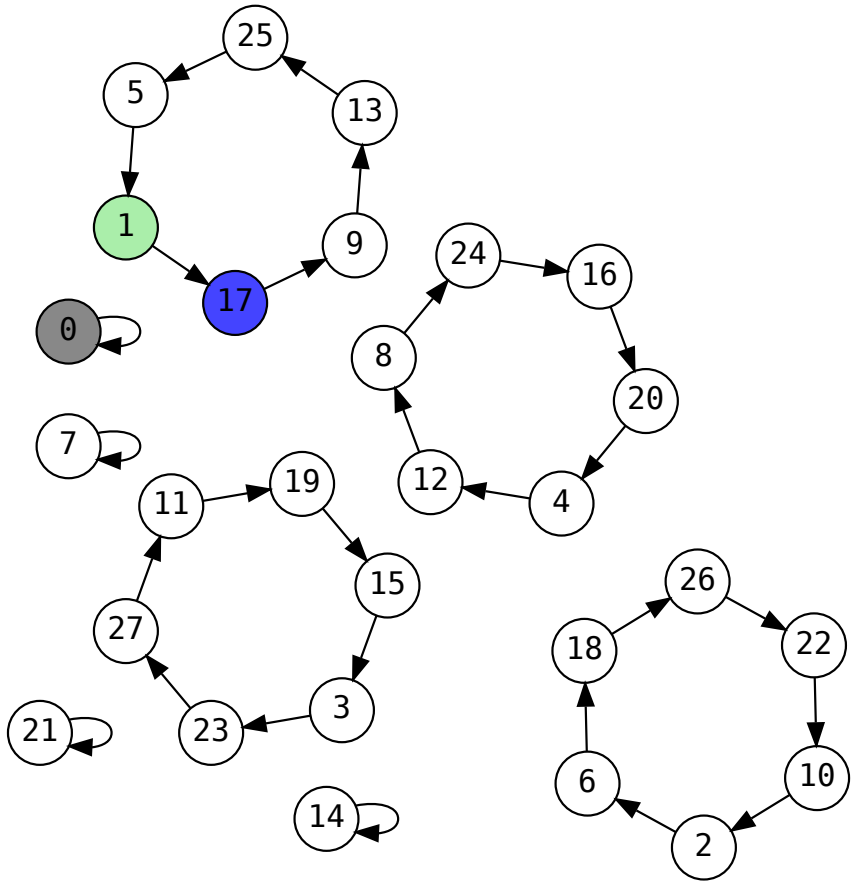
Multiplication, $n = 28, b = 15$



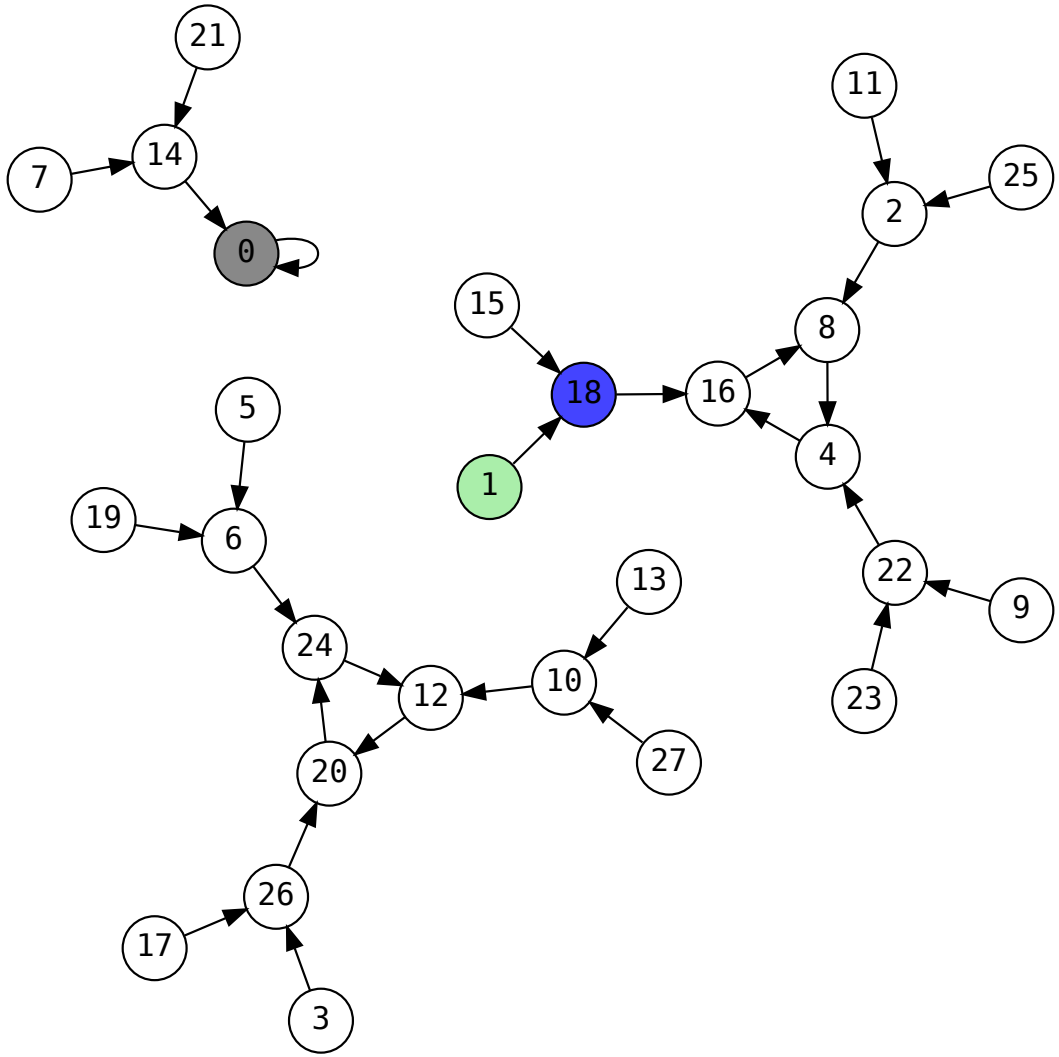
Multiplication, $n = 28, b = 16$



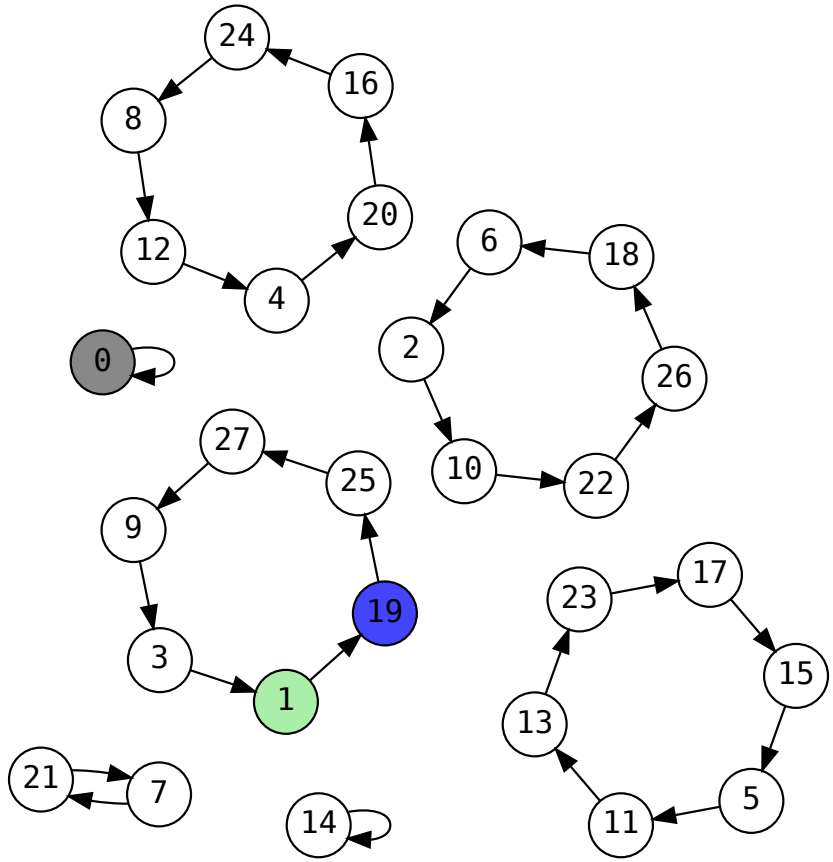
Multiplication, $n = 28, b = 17$



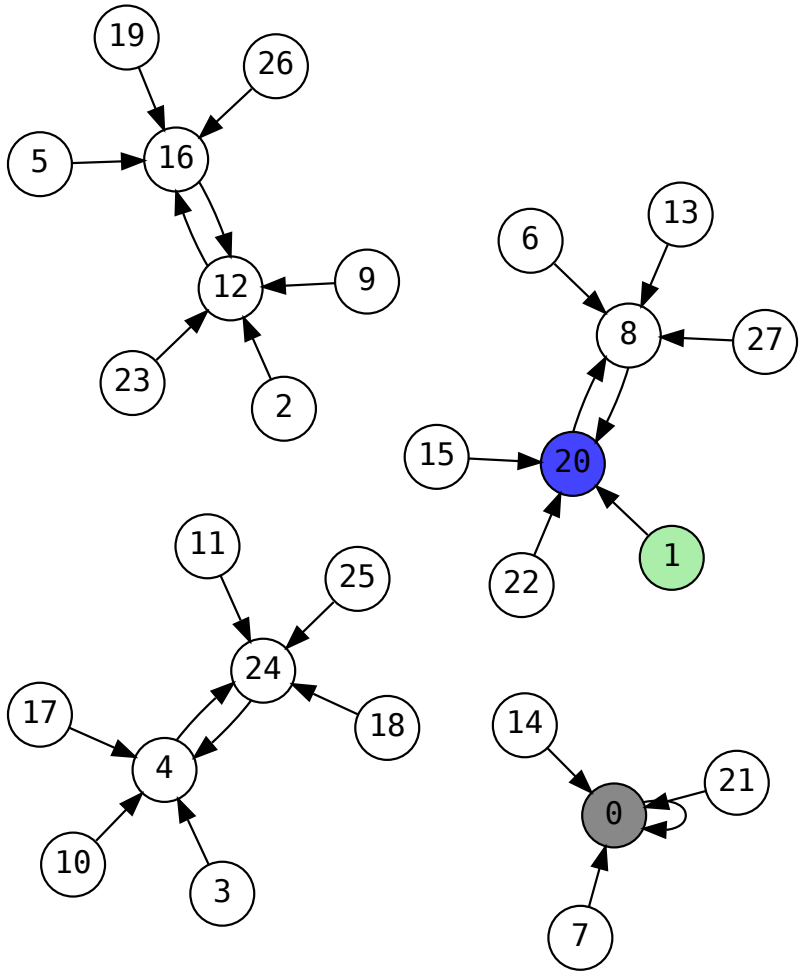
Multiplication, $n = 28, b = 18$



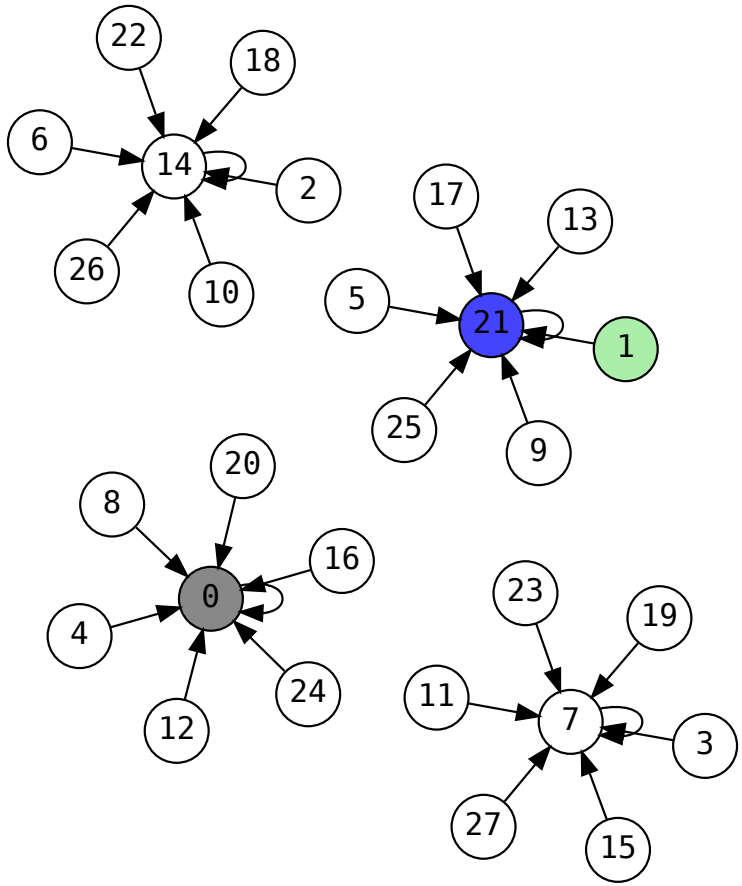
Multiplication, $n = 28, b = 19$



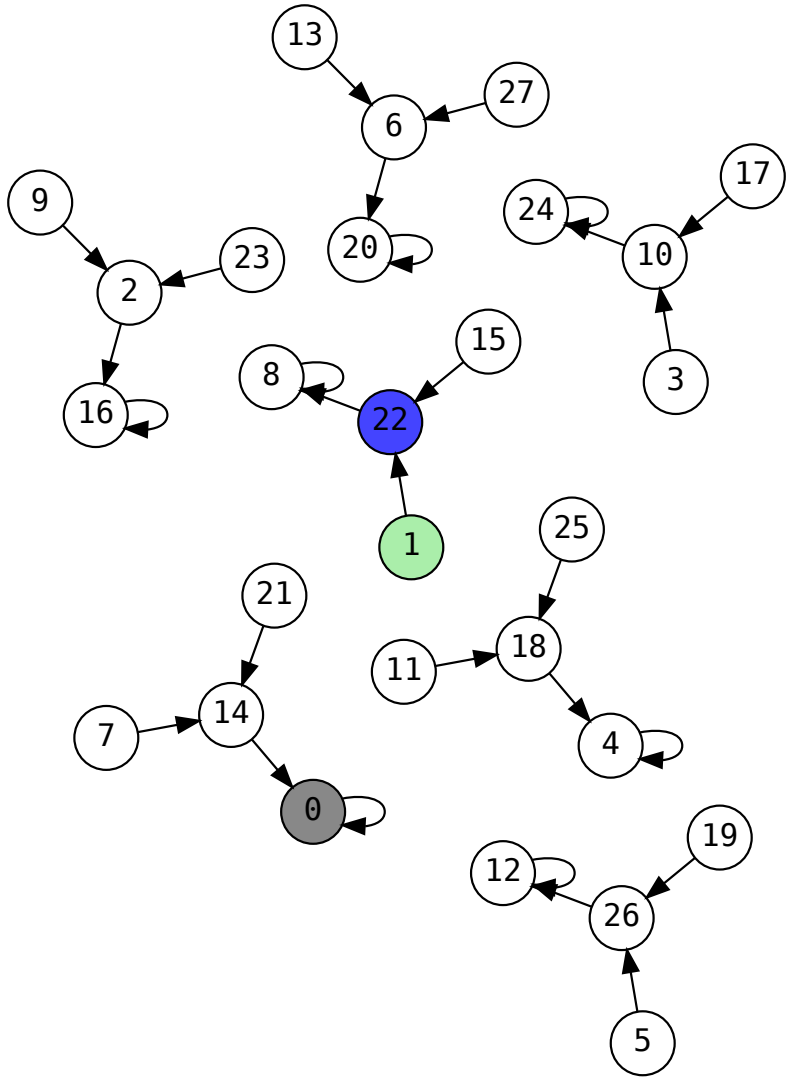
Multiplication, $n = 28, b = 20$



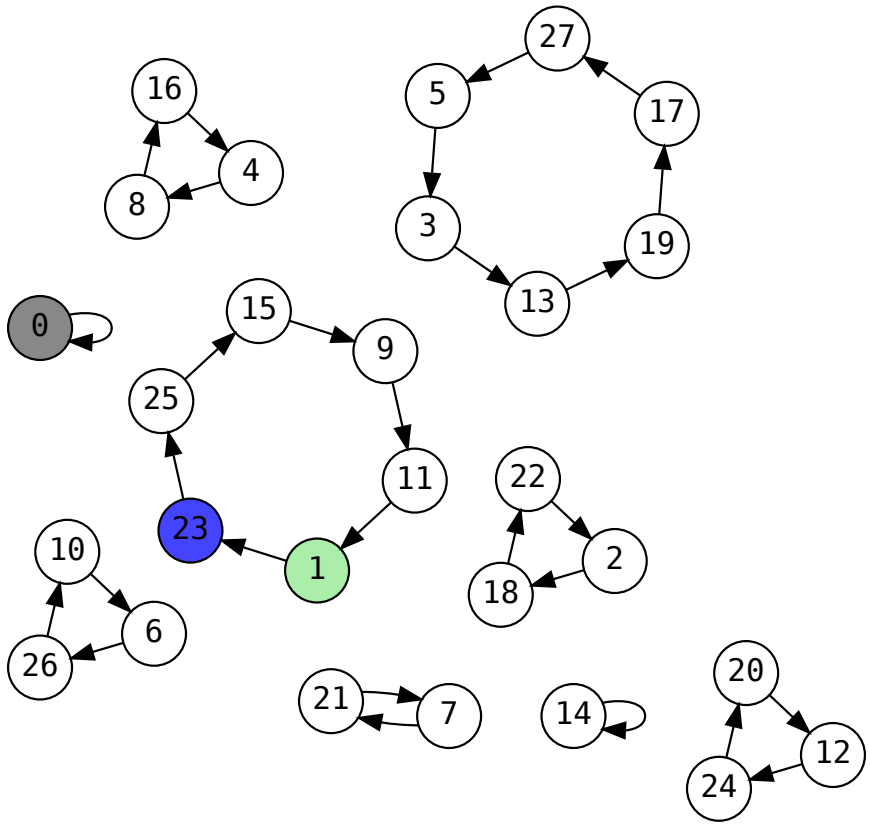
Multiplication, $n = 28, b = 21$



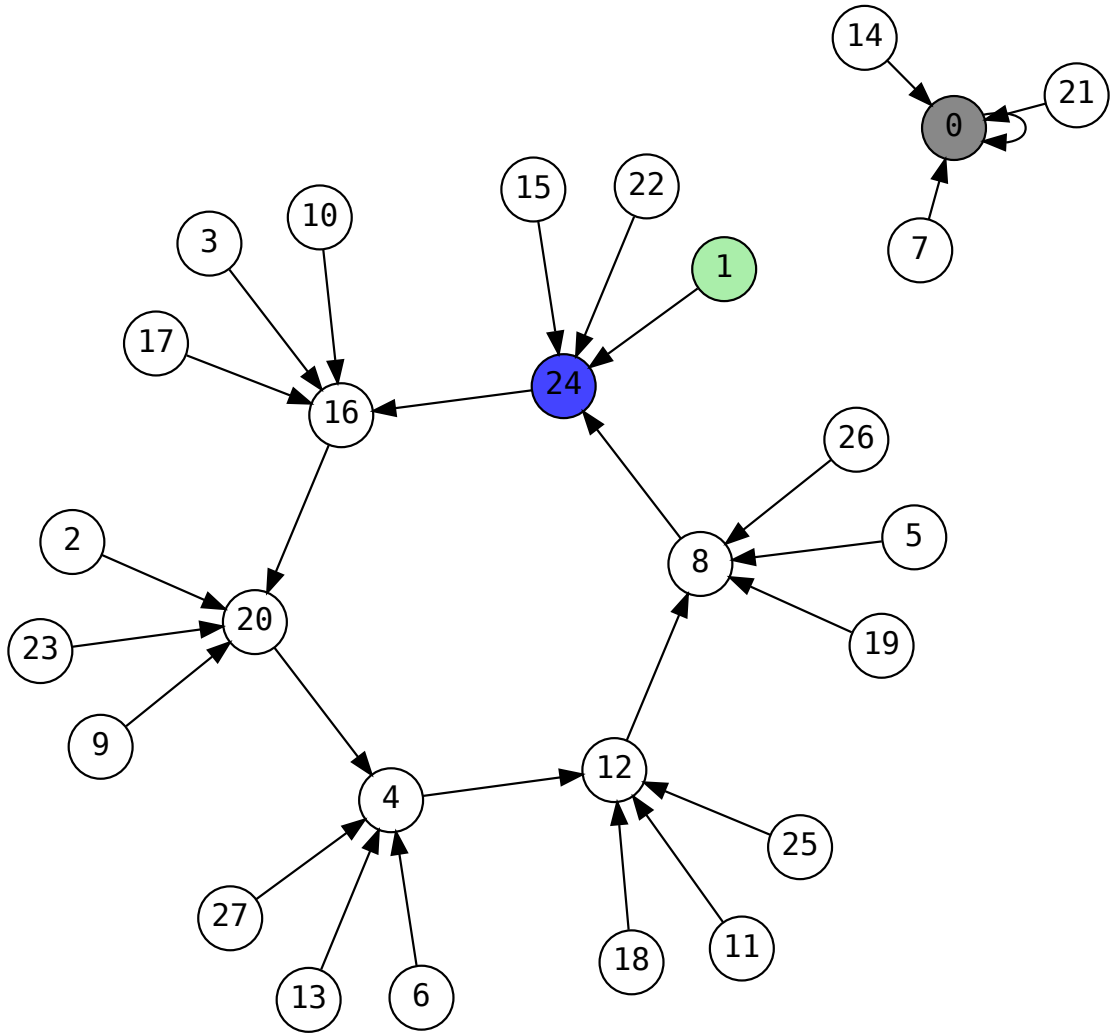
Multiplication, $n = 28, b = 22$



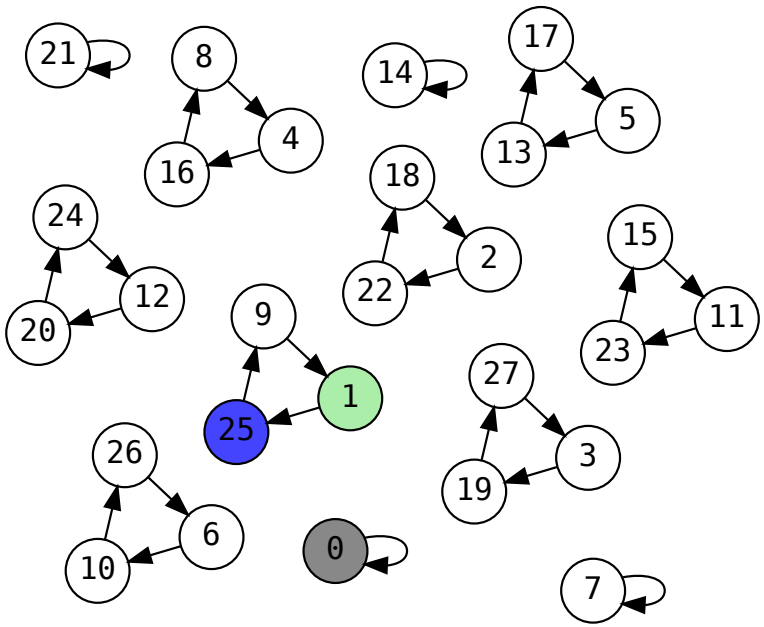
Multiplication, $n = 28, b = 23$



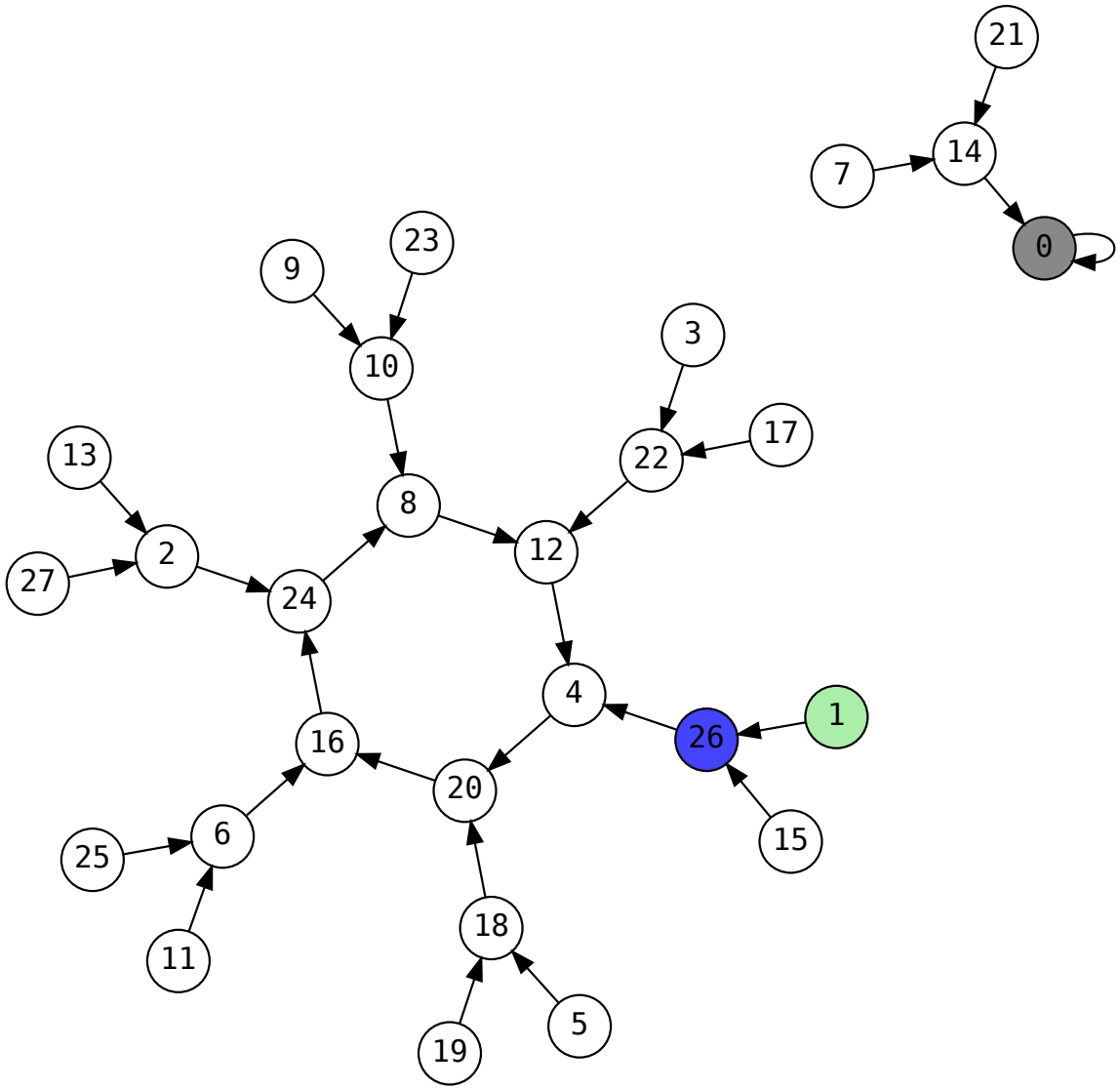
Multiplication, $n = 28, b = 24$



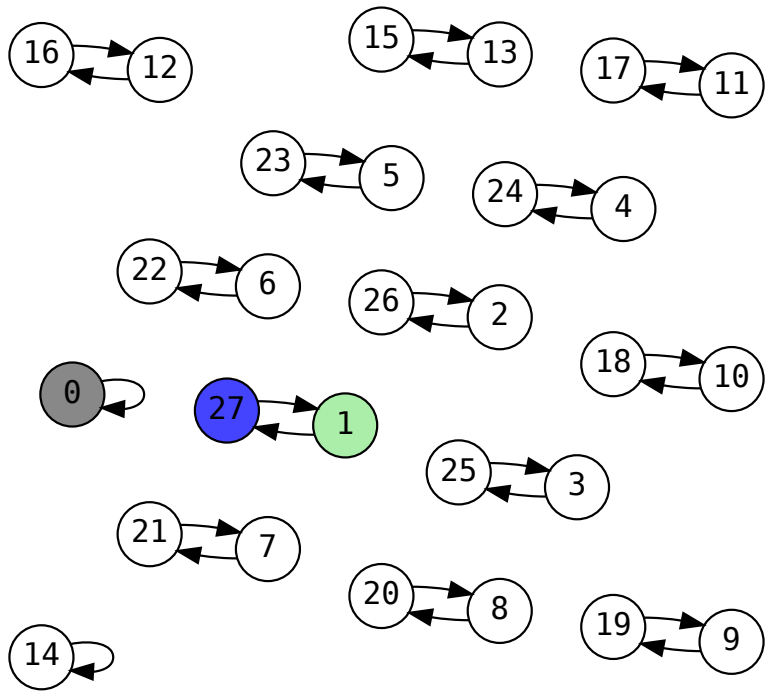
Multiplication, $n = 28, b = 25$



Multiplication, $n = 28, b = 26$

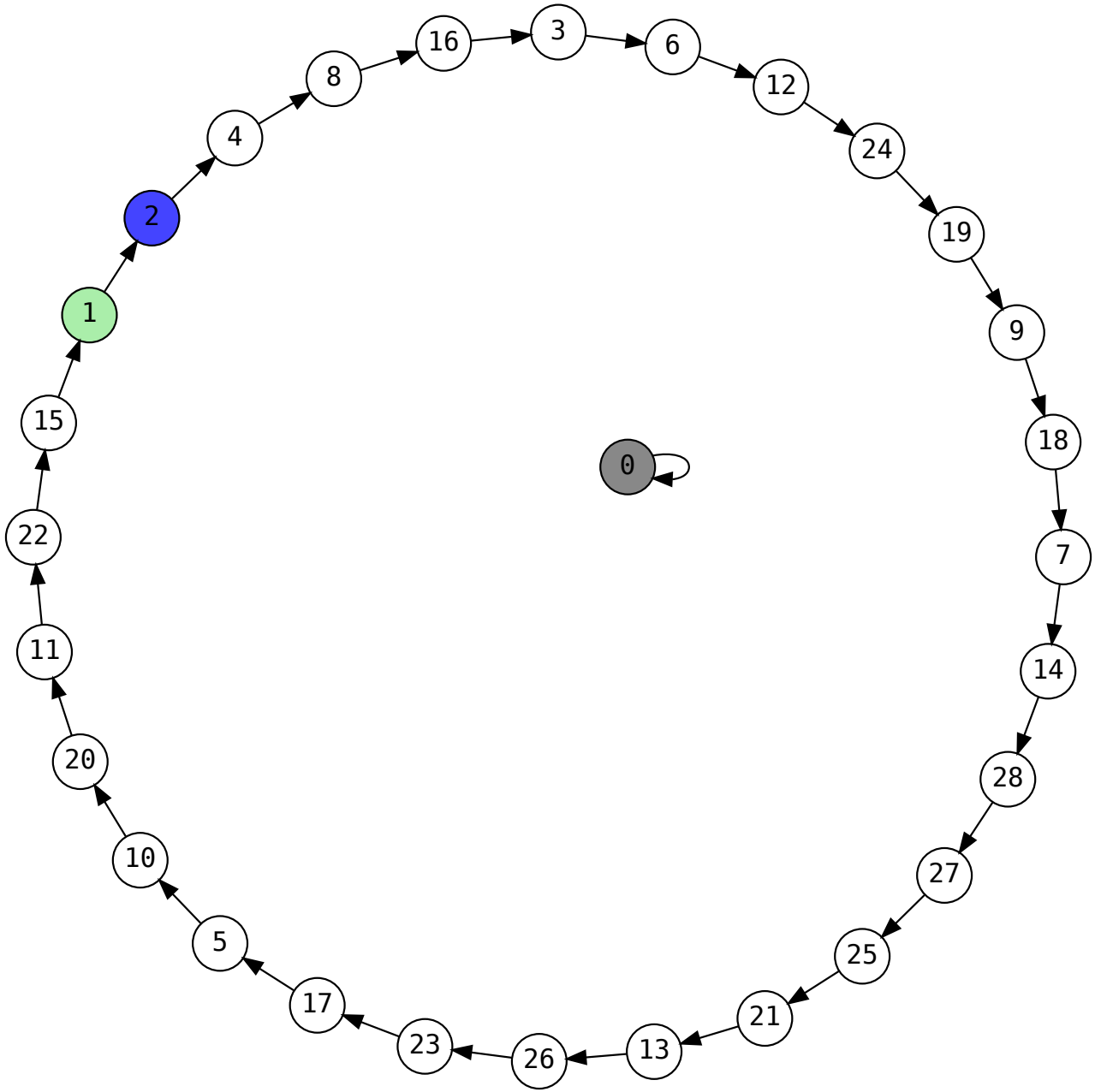


Multiplication, $n = 28, b = 27$

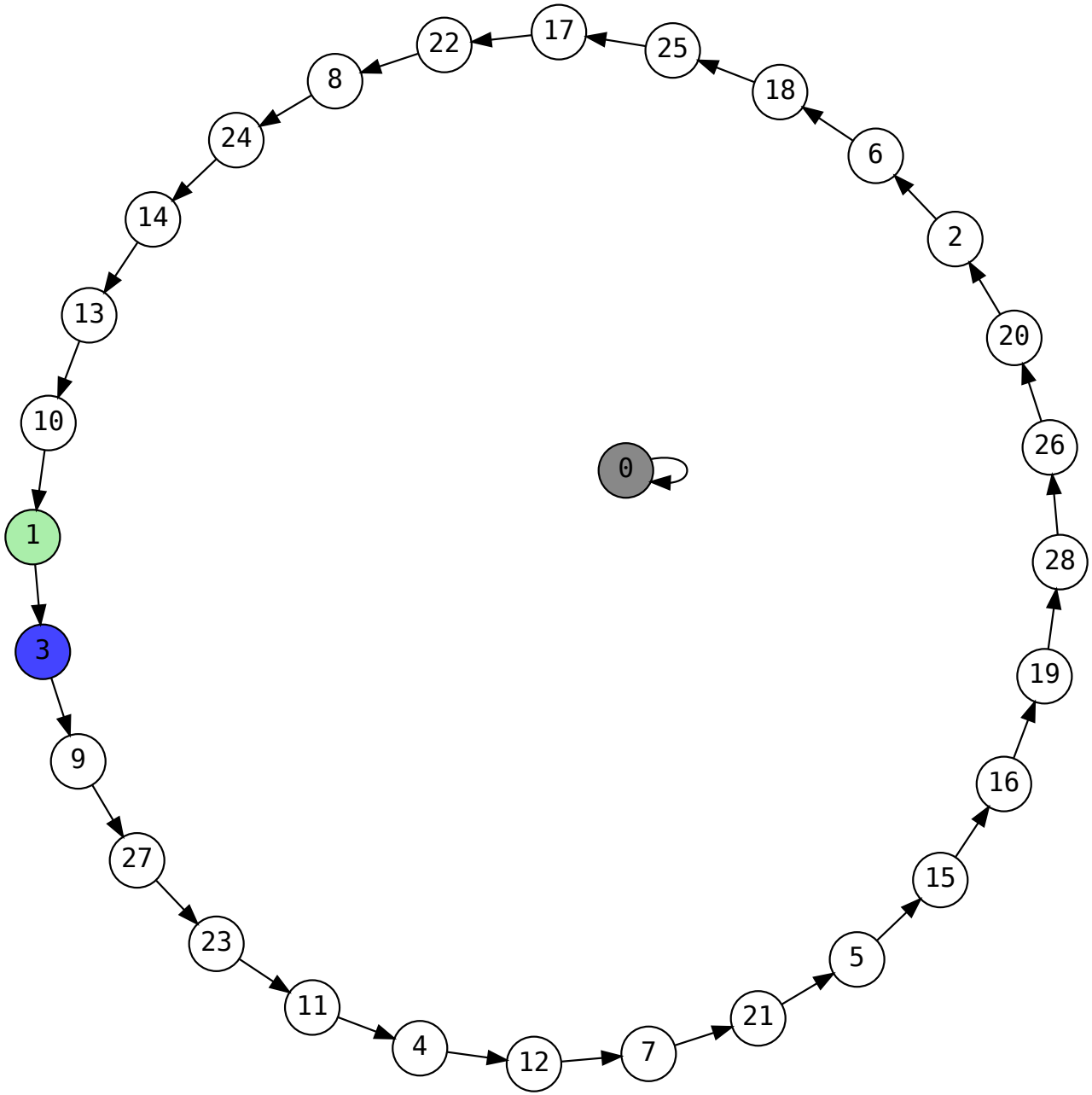


Multiplication, $n = 29$

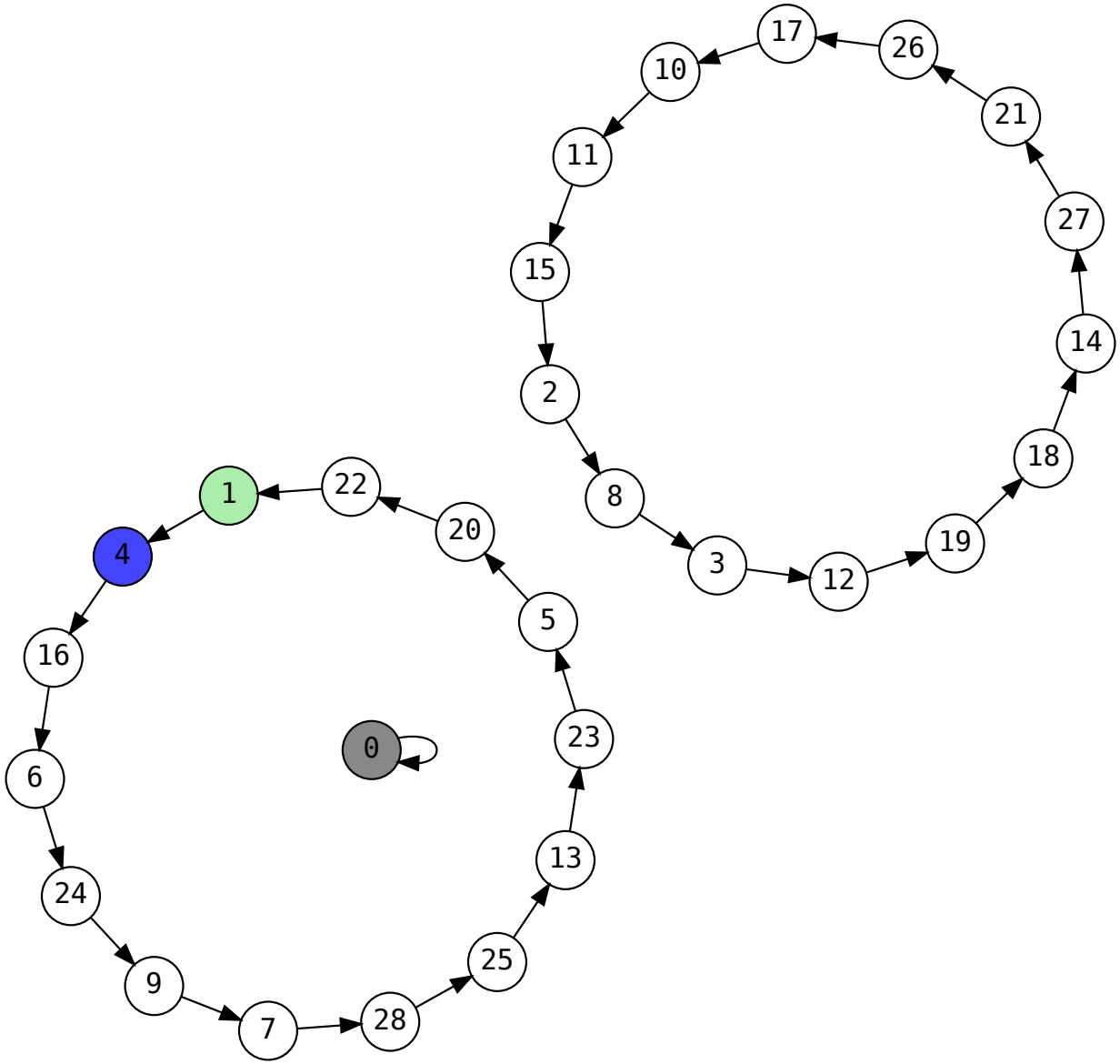
Multiplication, $n = 29, b = 2$



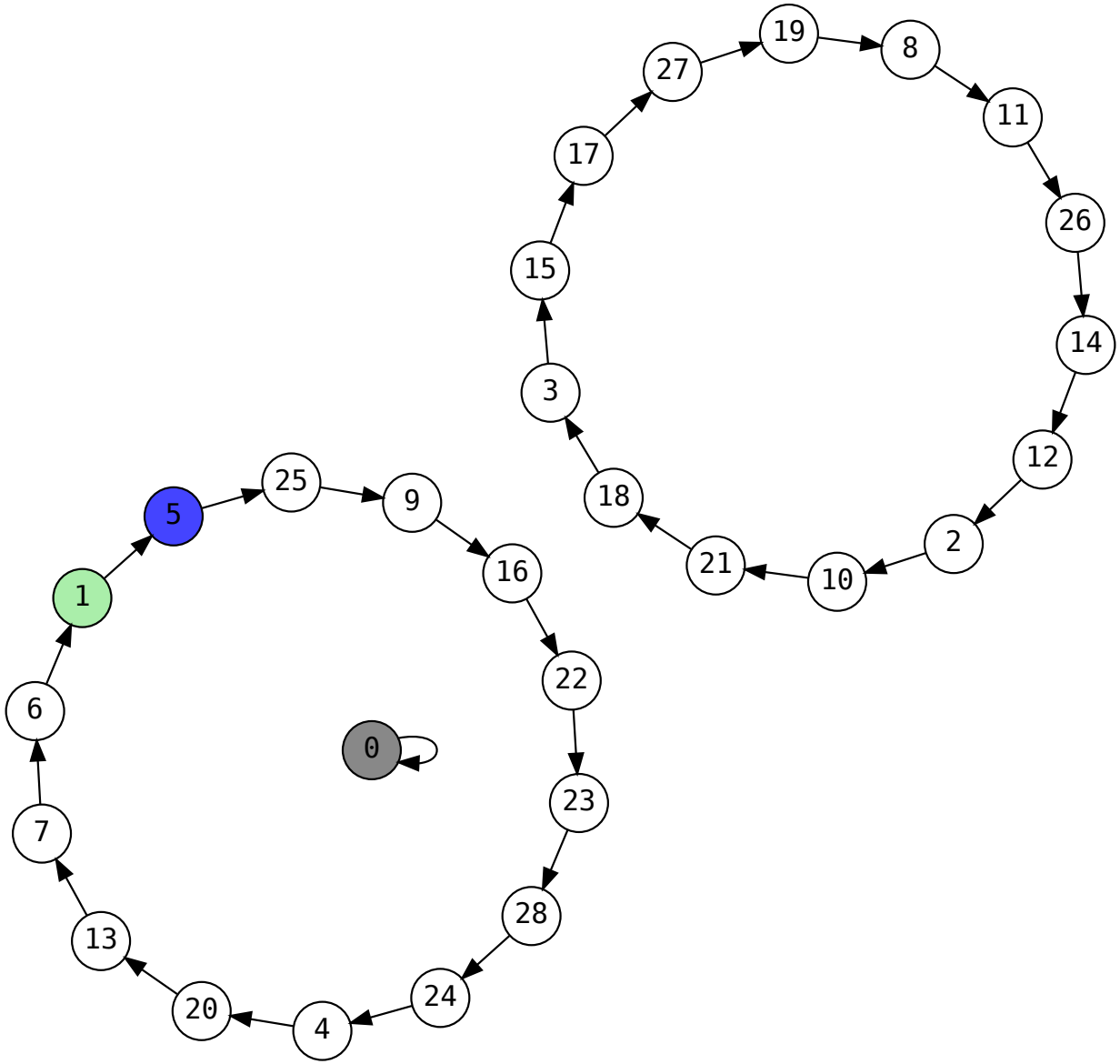
Multiplication, $n = 29, b = 3$



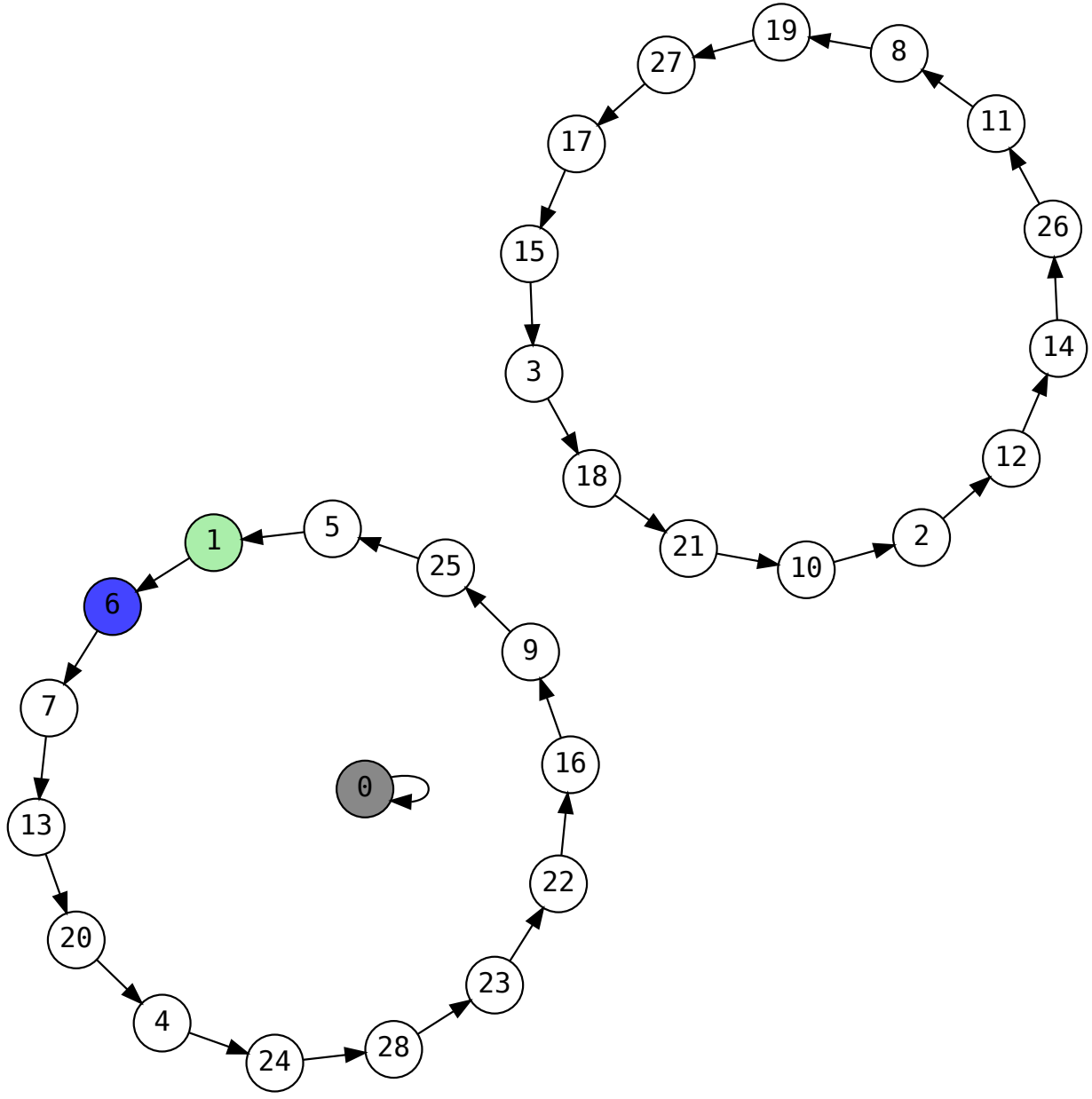
Multiplication, $n = 29, b = 4$



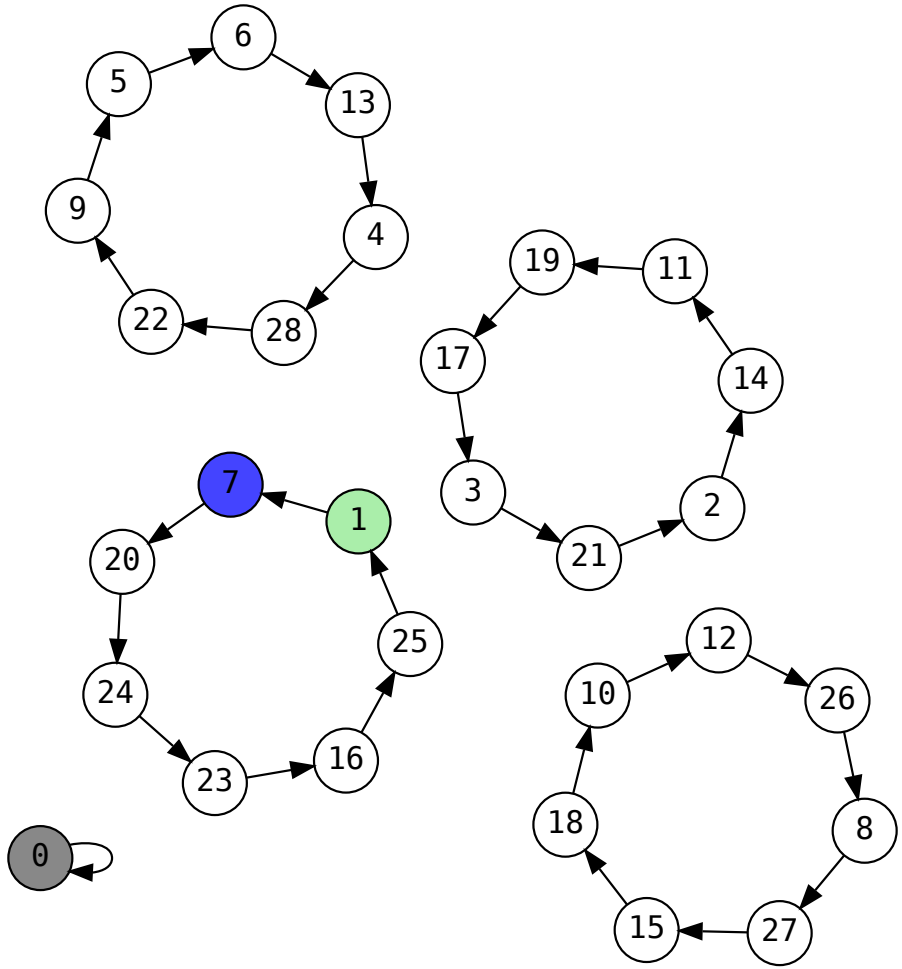
Multiplication, $n = 29, b = 5$



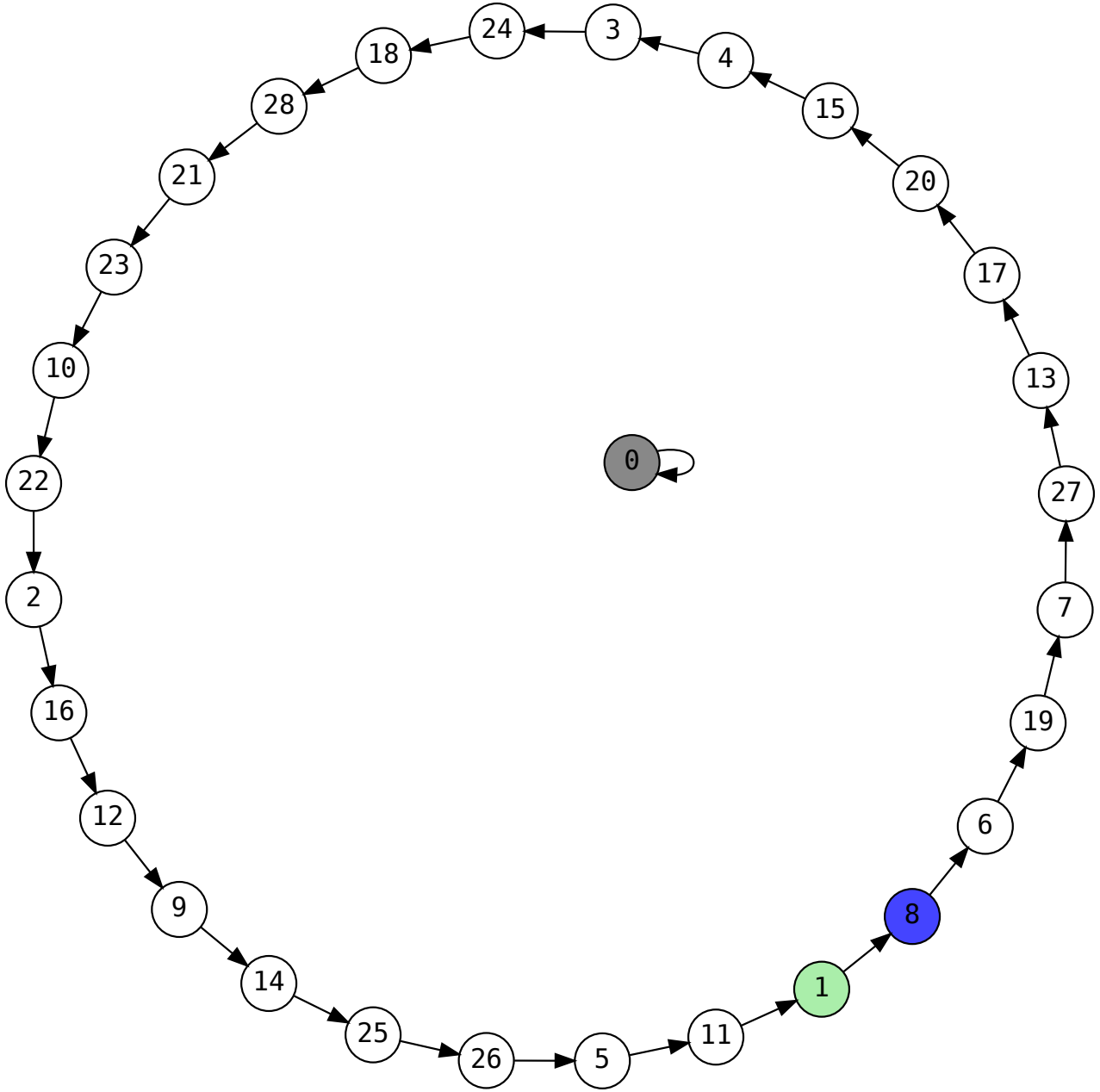
Multiplication, $n = 29, b = 6$



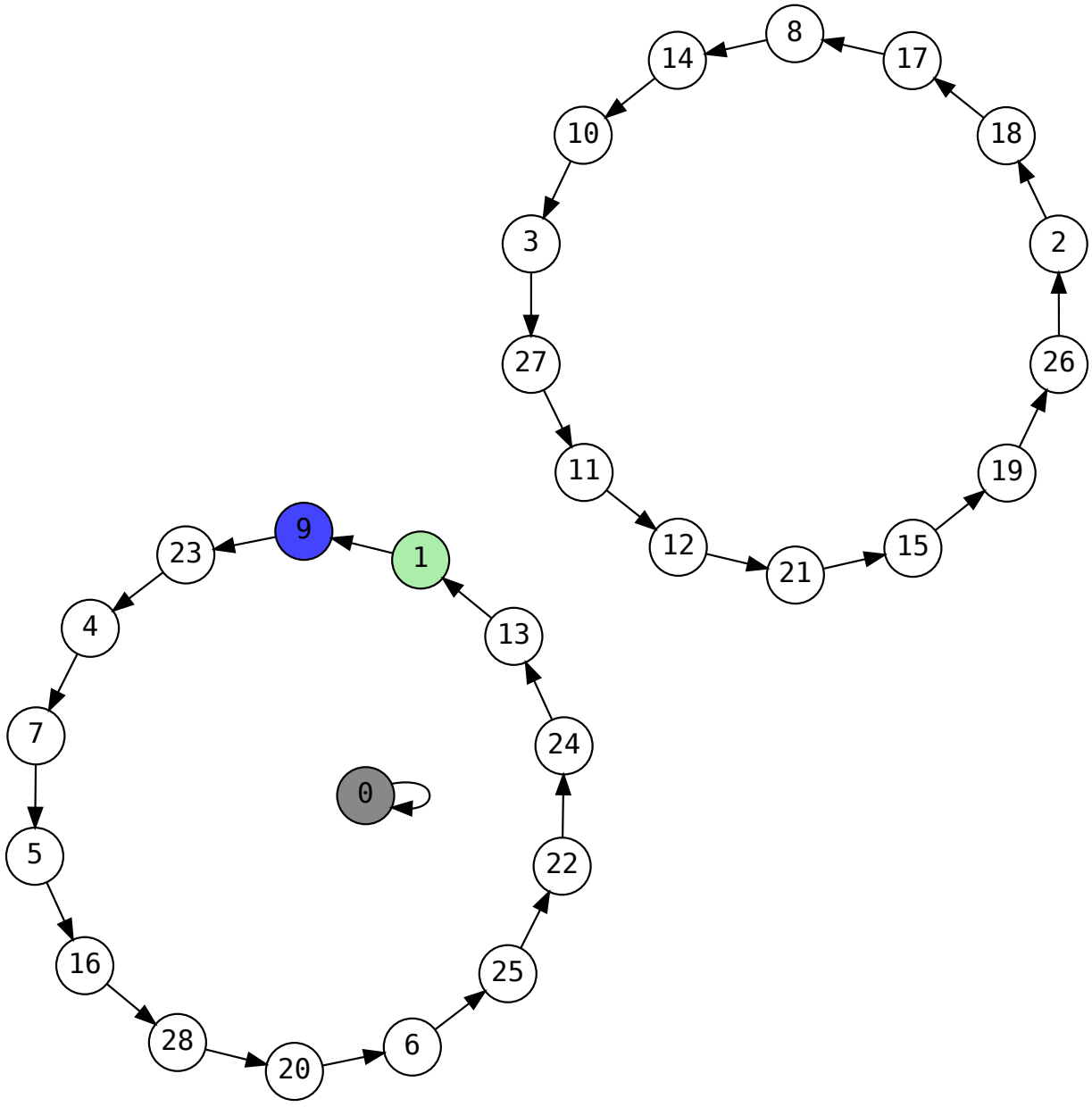
Multiplication, $n = 29, b = 7$



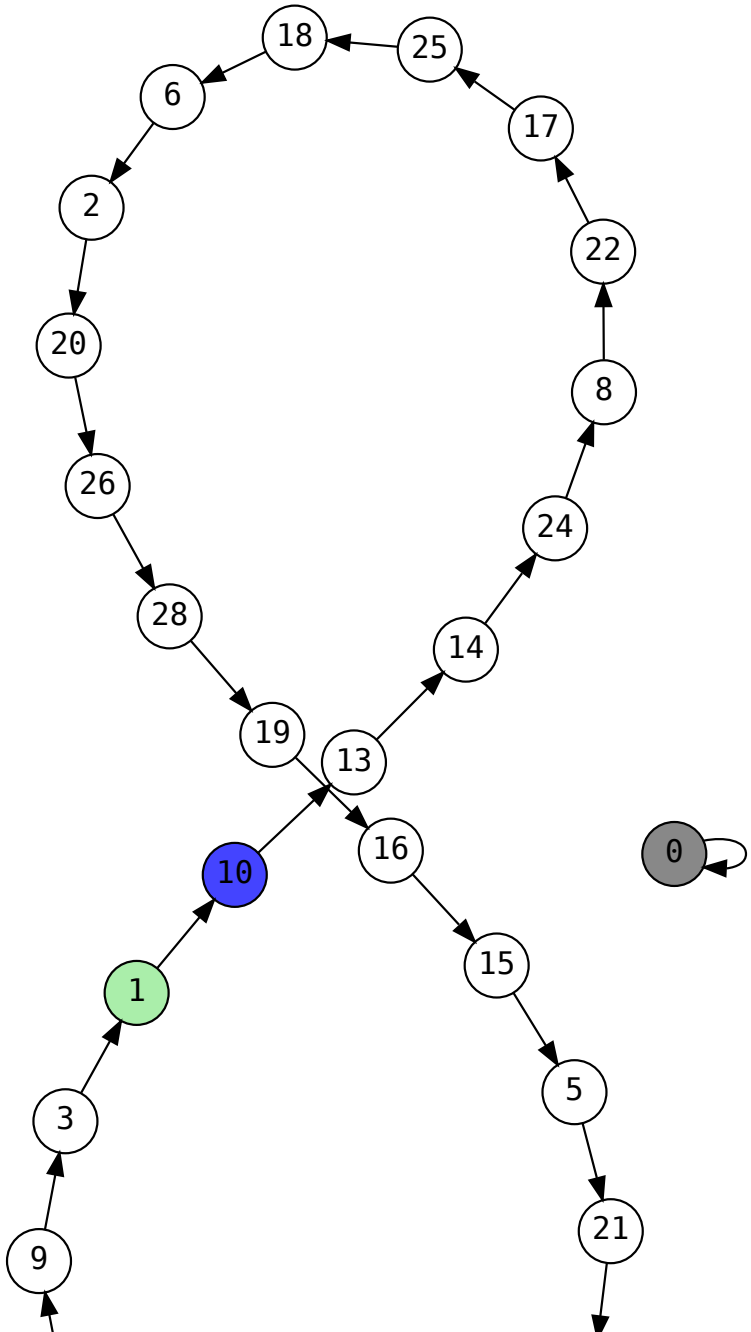
Multiplication, $n = 29, b = 8$



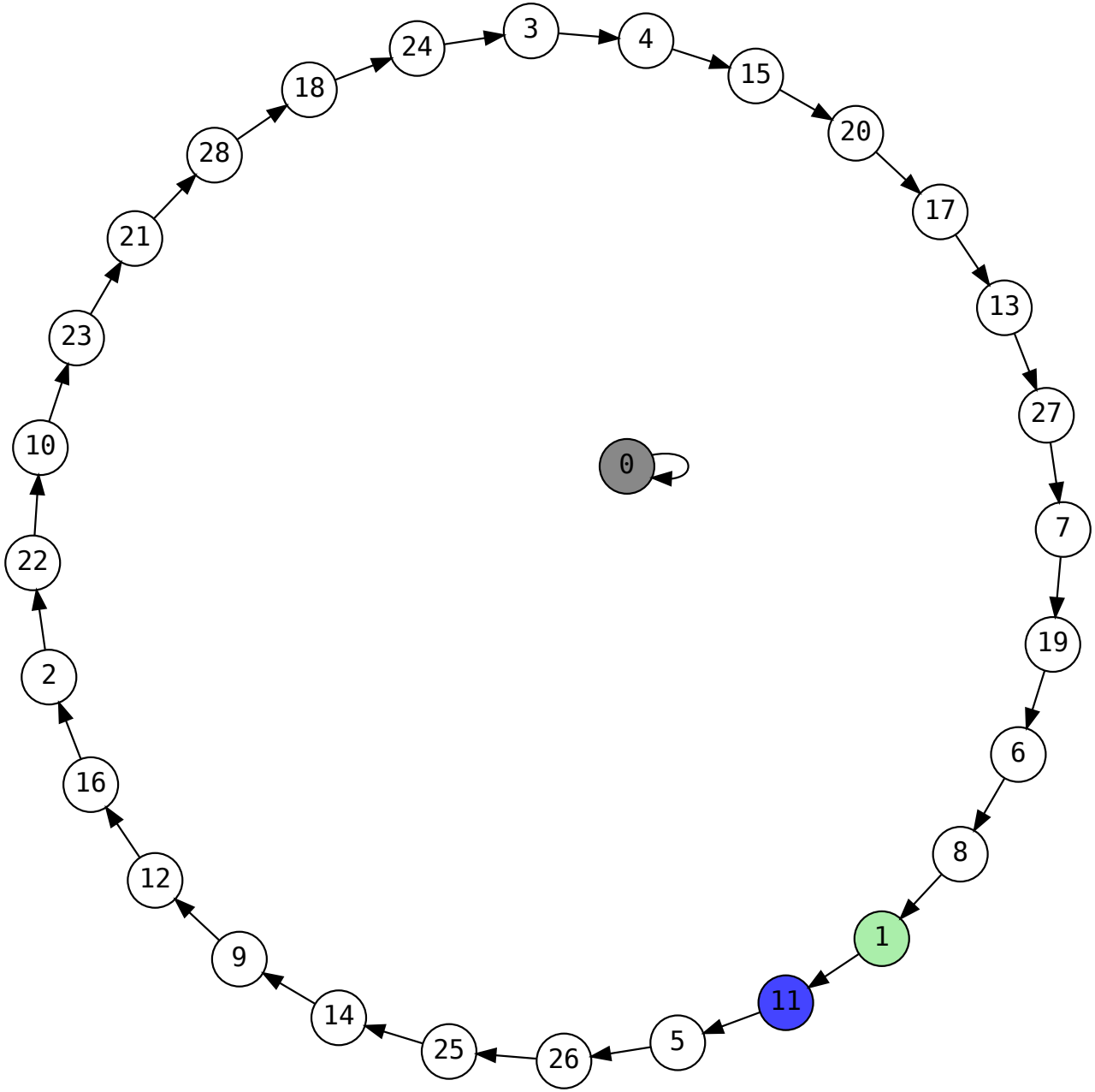
Multiplication, $n = 29, b = 9$



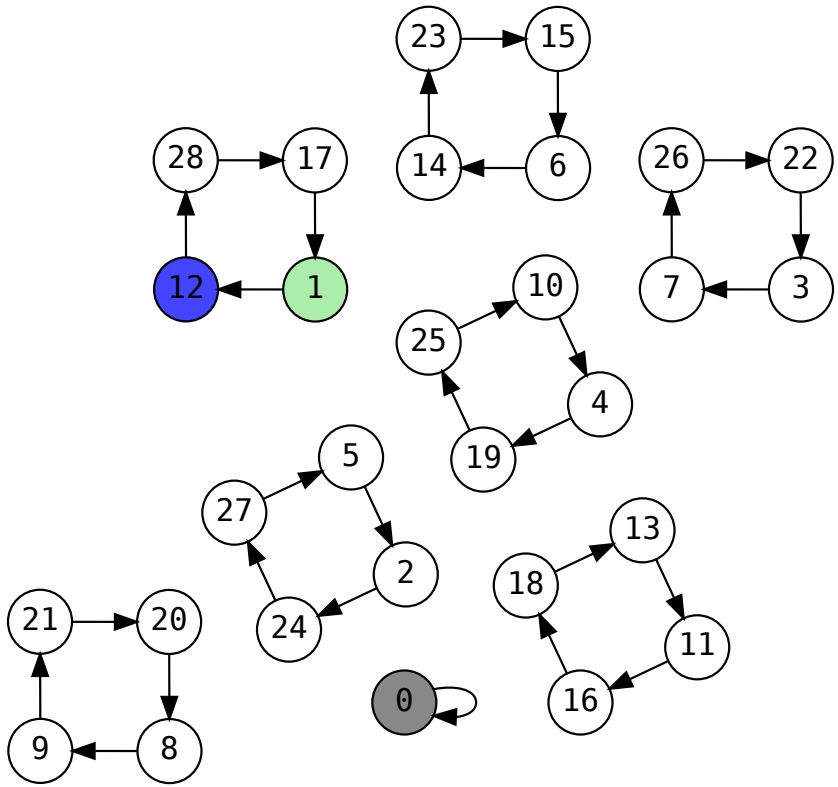
Multiplication, $n = 29, b = 10$



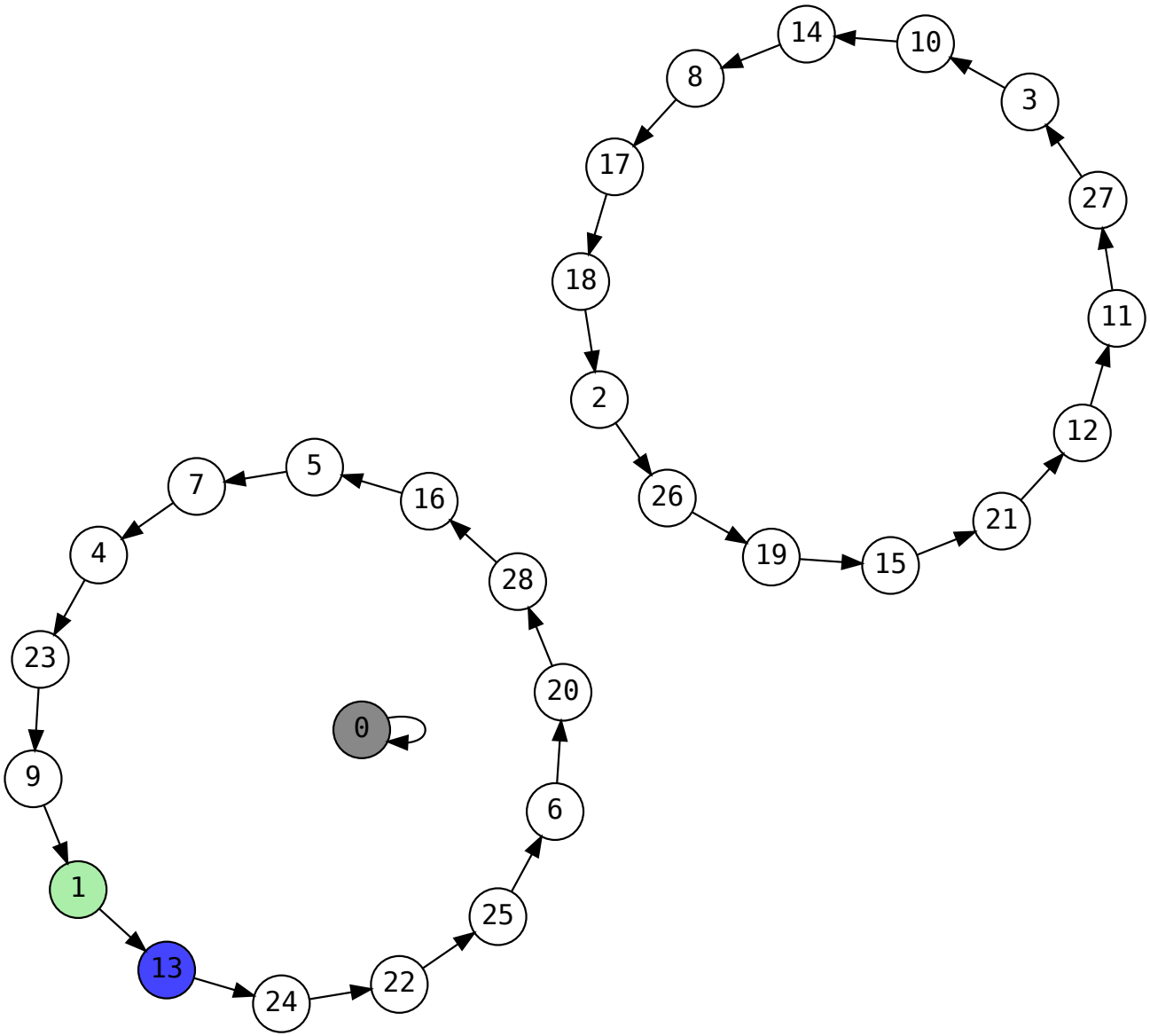
Multiplication, $n = 29, b = 11$



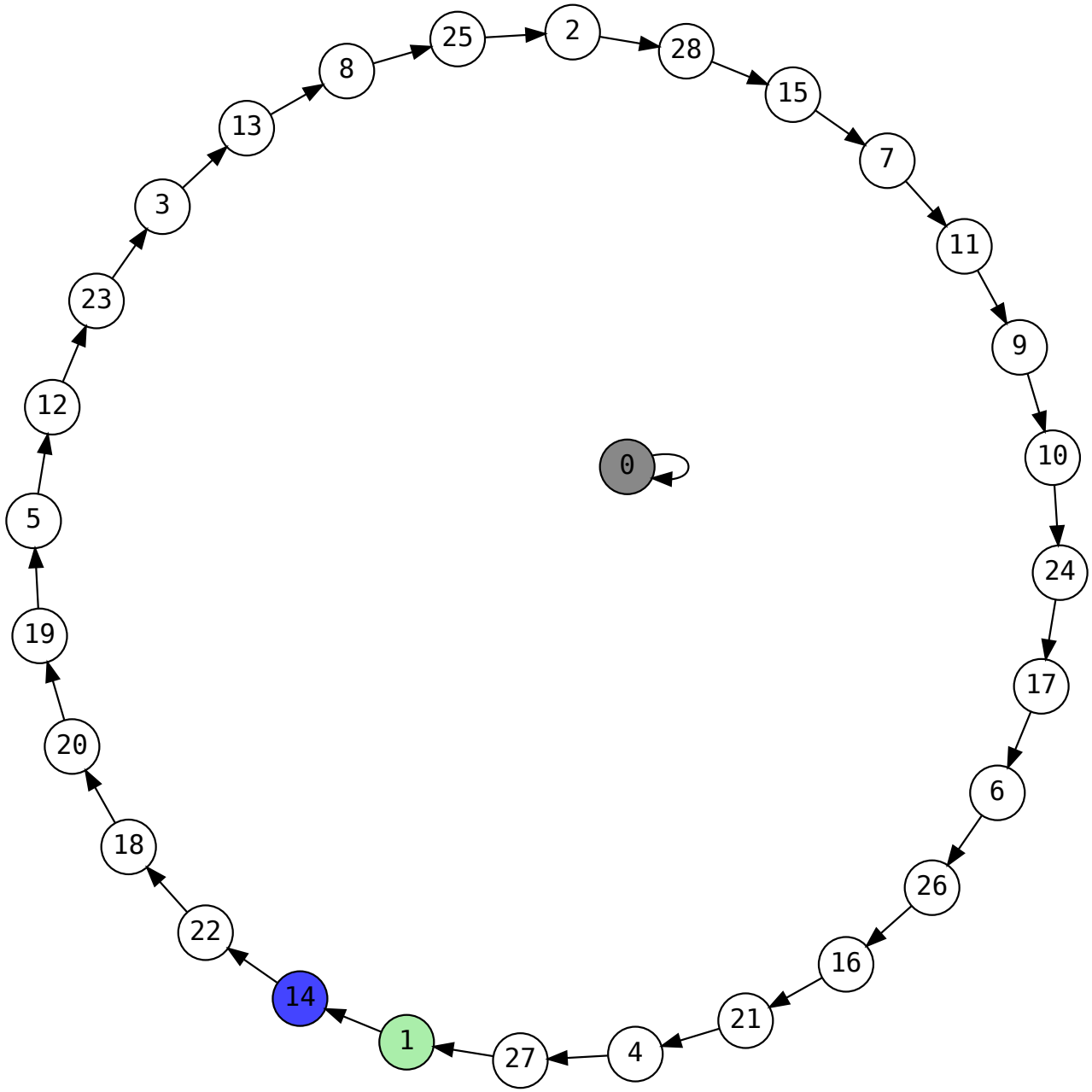
Multiplication, $n = 29, b = 12$



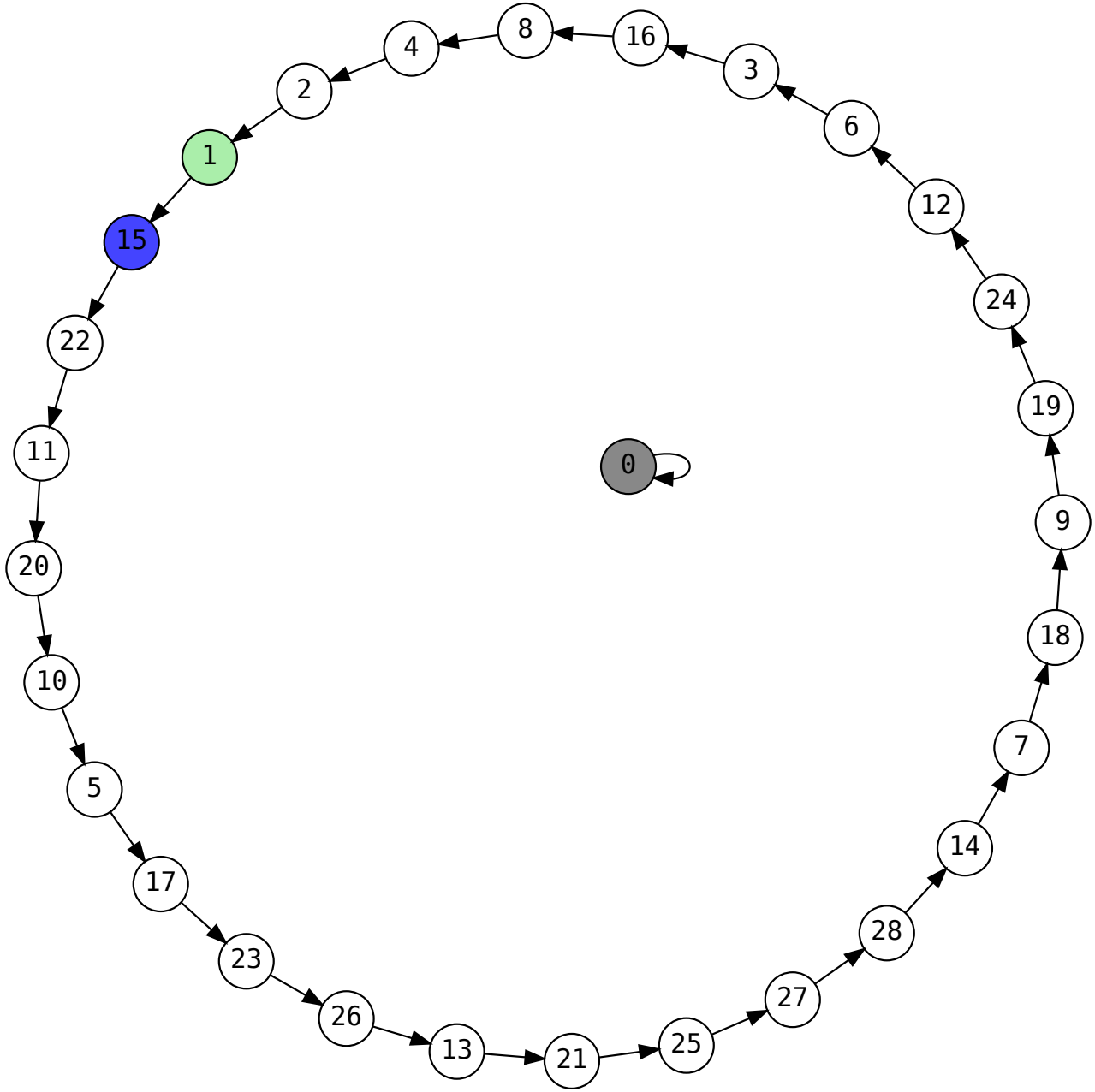
Multiplication, $n = 29, b = 13$



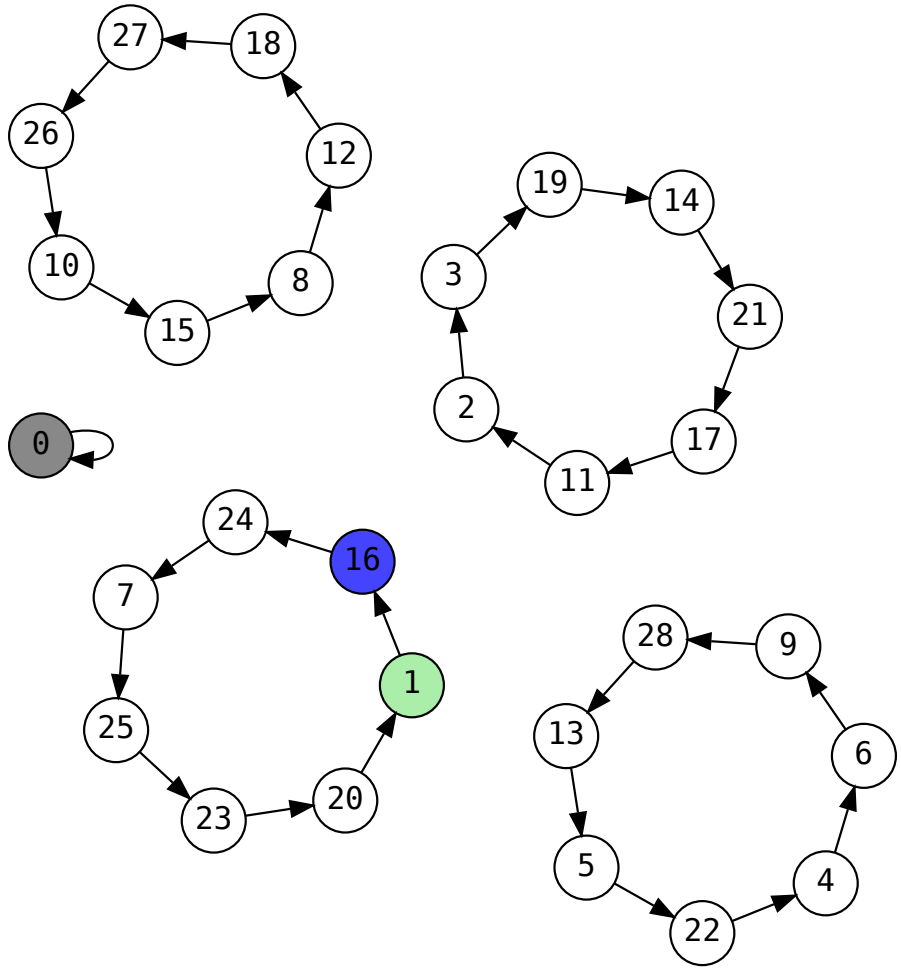
Multiplication, $n = 29, b = 14$



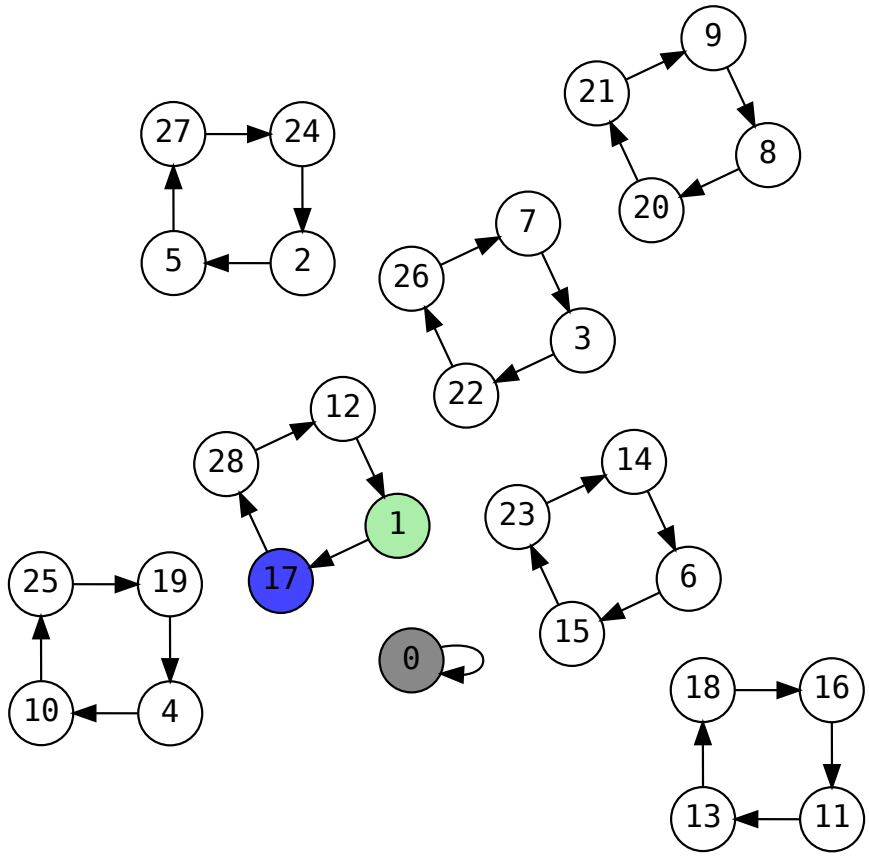
Multiplication, $n = 29, b = 15$



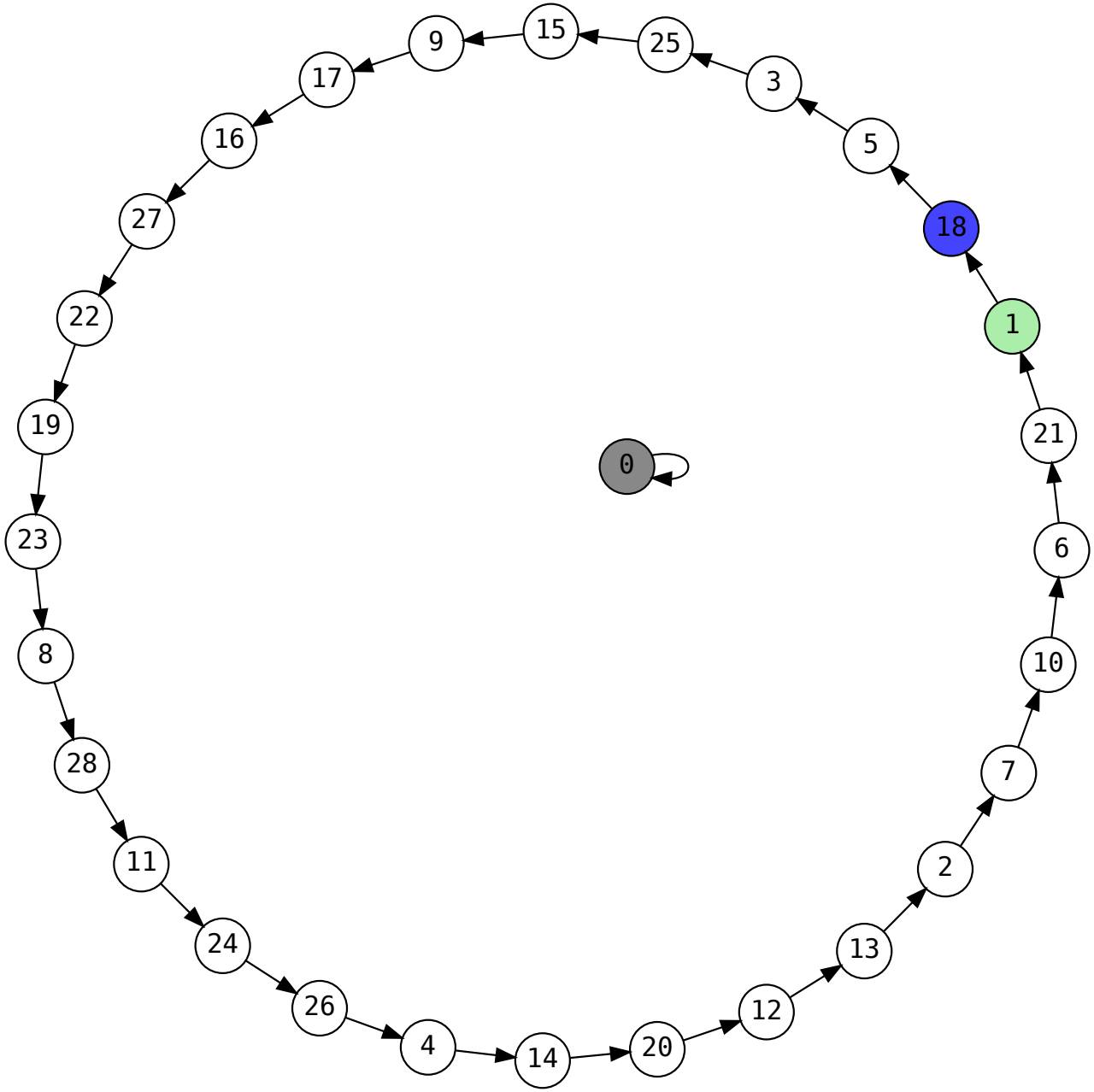
Multiplication, $n = 29, b = 16$



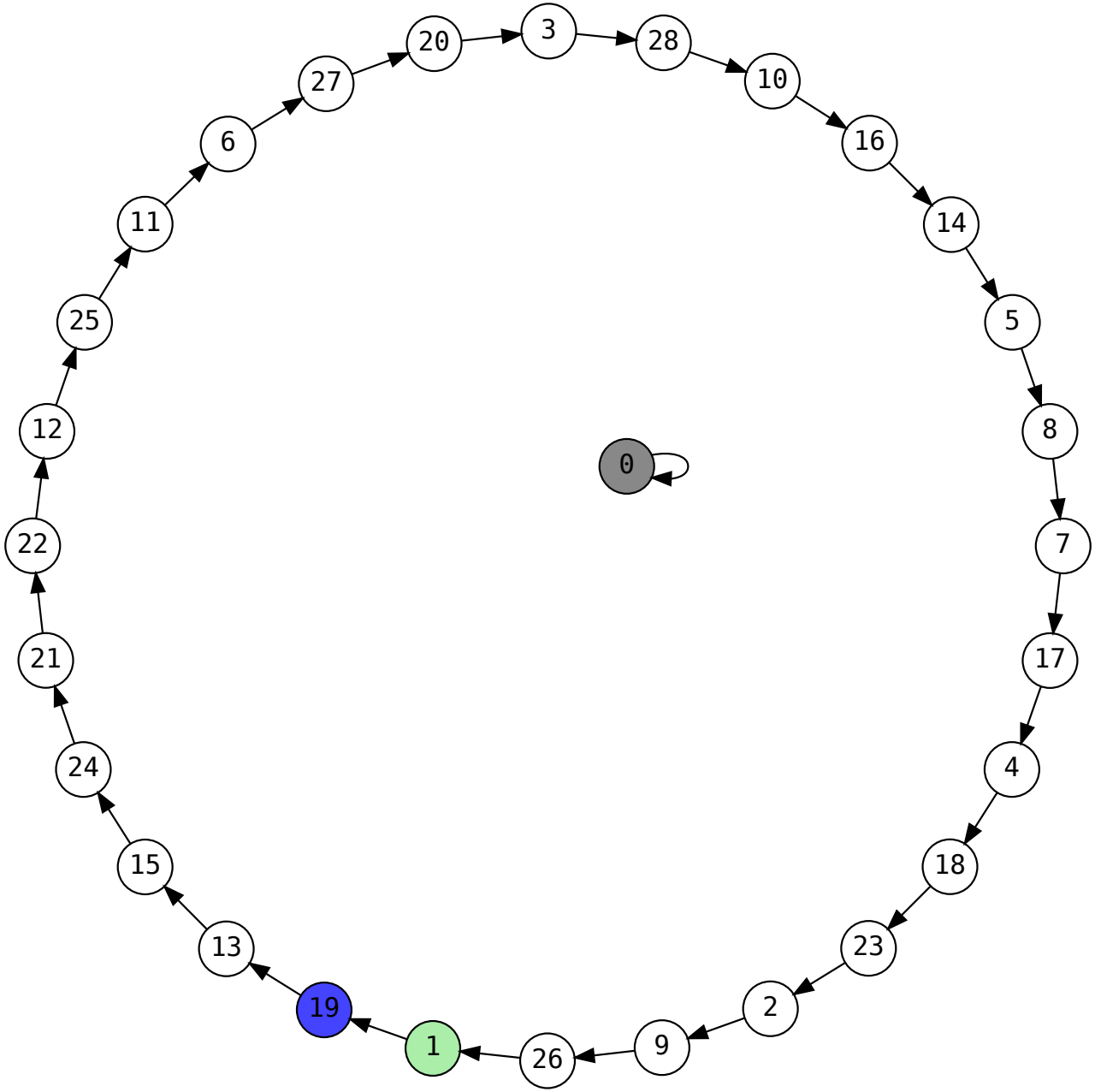
Multiplication, $n = 29, b = 17$



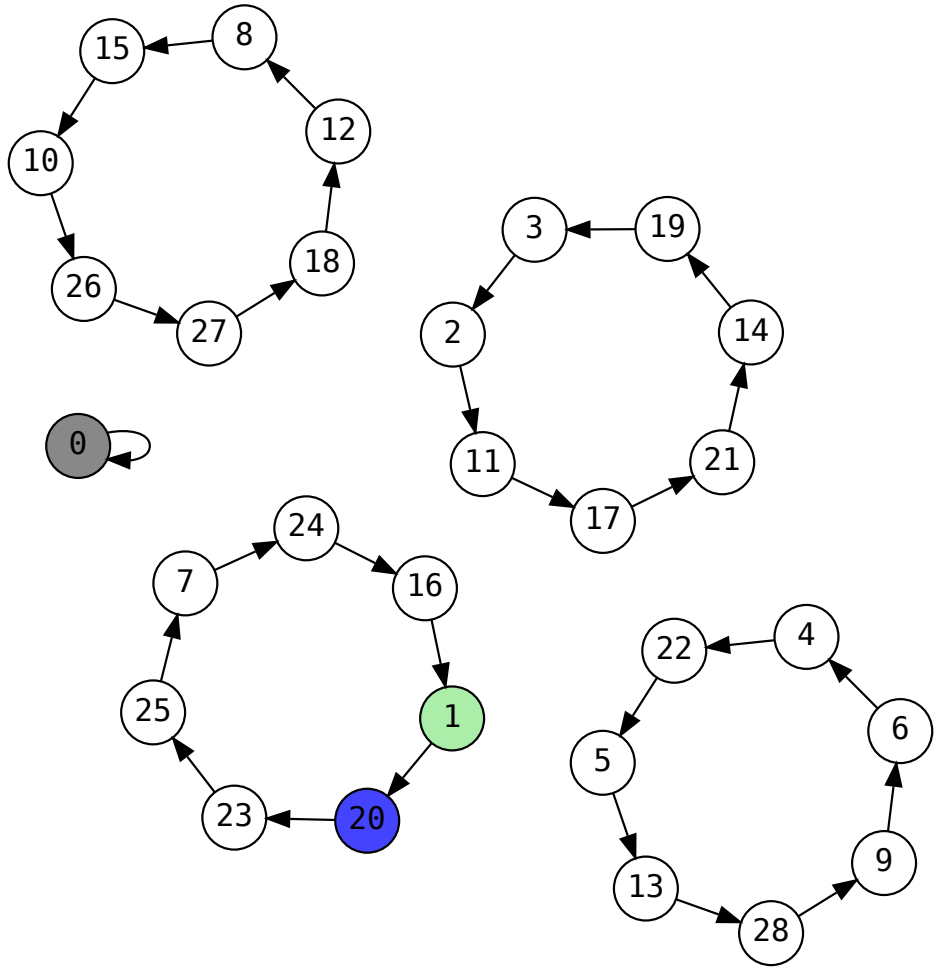
Multiplication, $n = 29, b = 18$



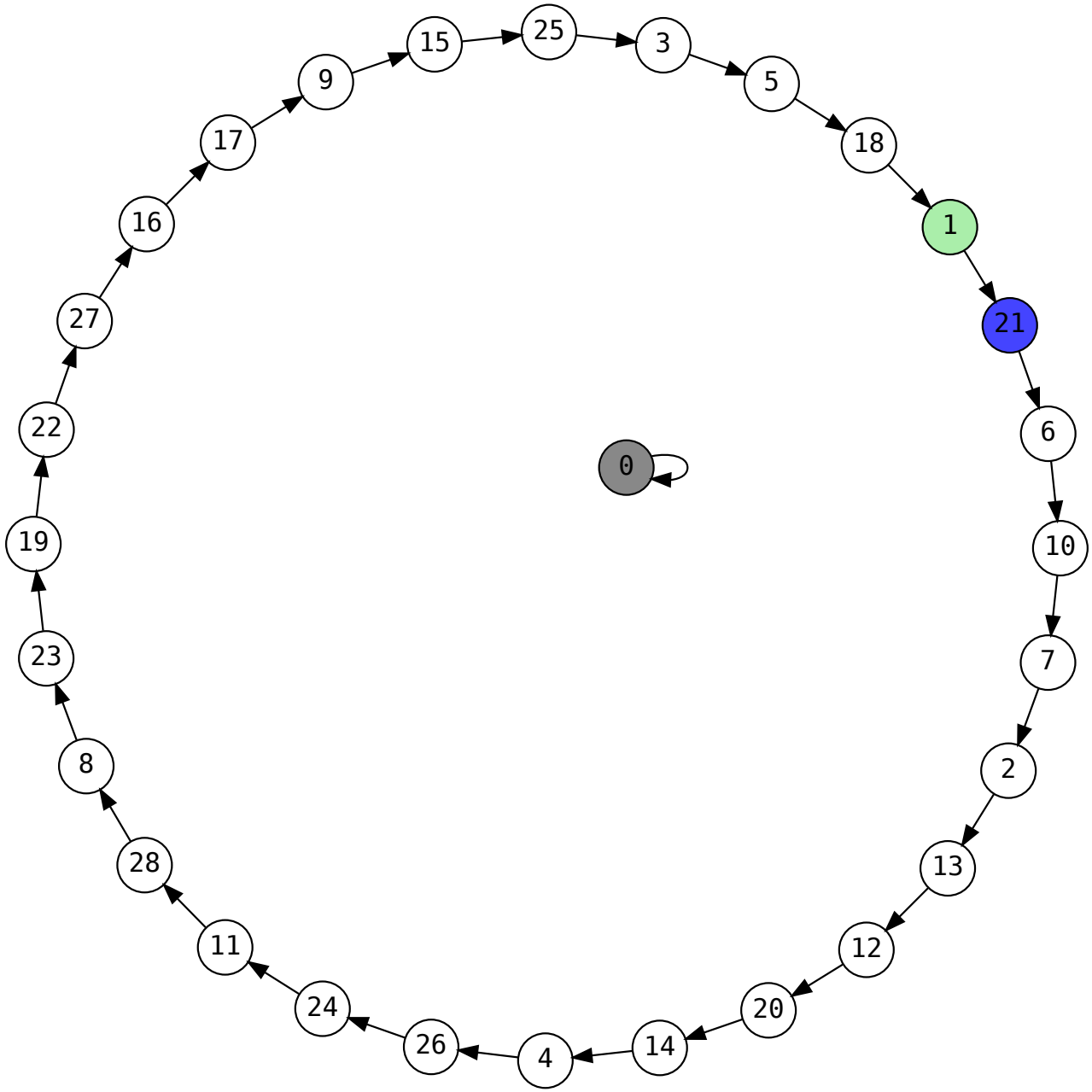
Multiplication, $n = 29, b = 19$



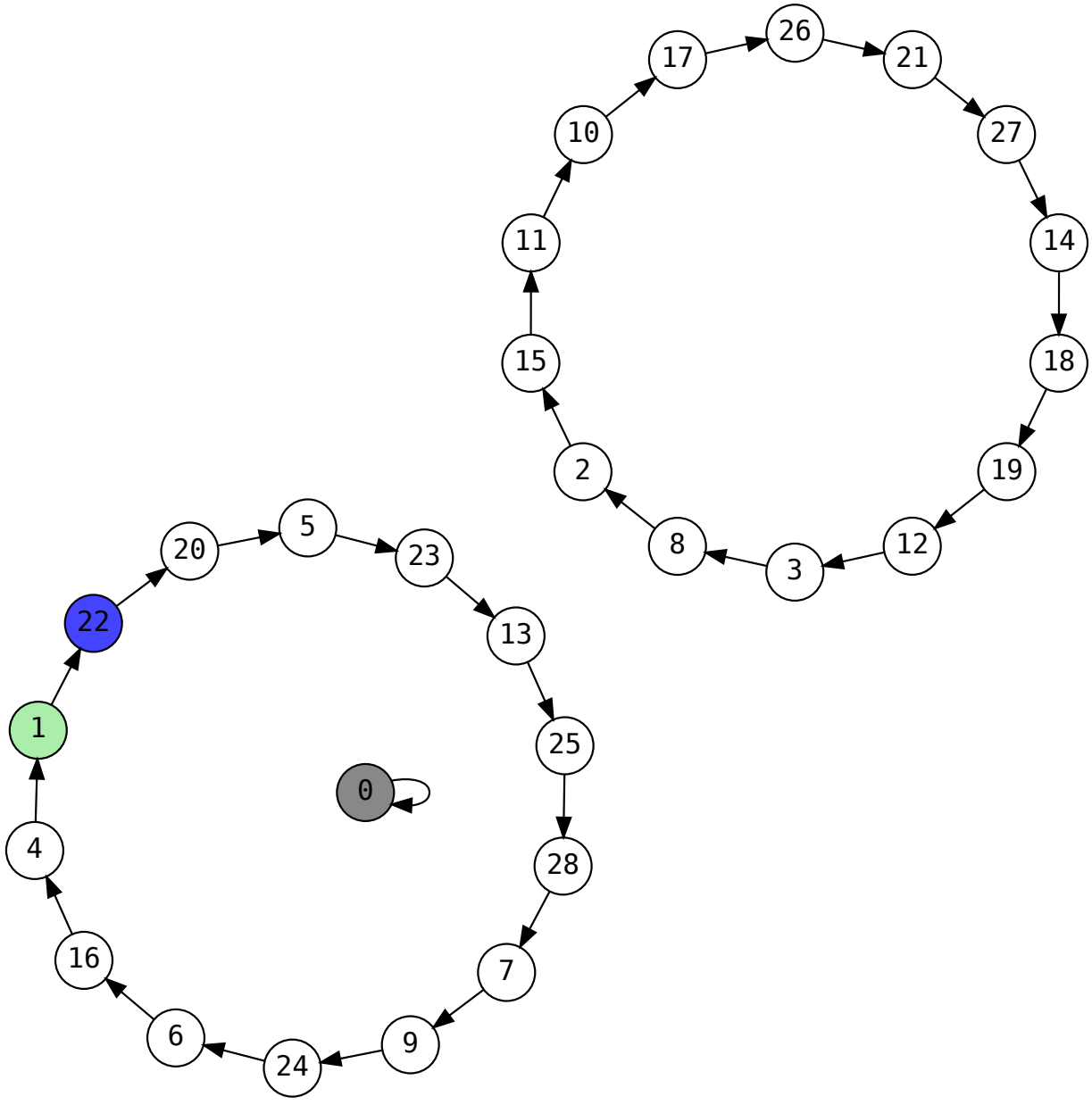
Multiplication, $n = 29, b = 20$



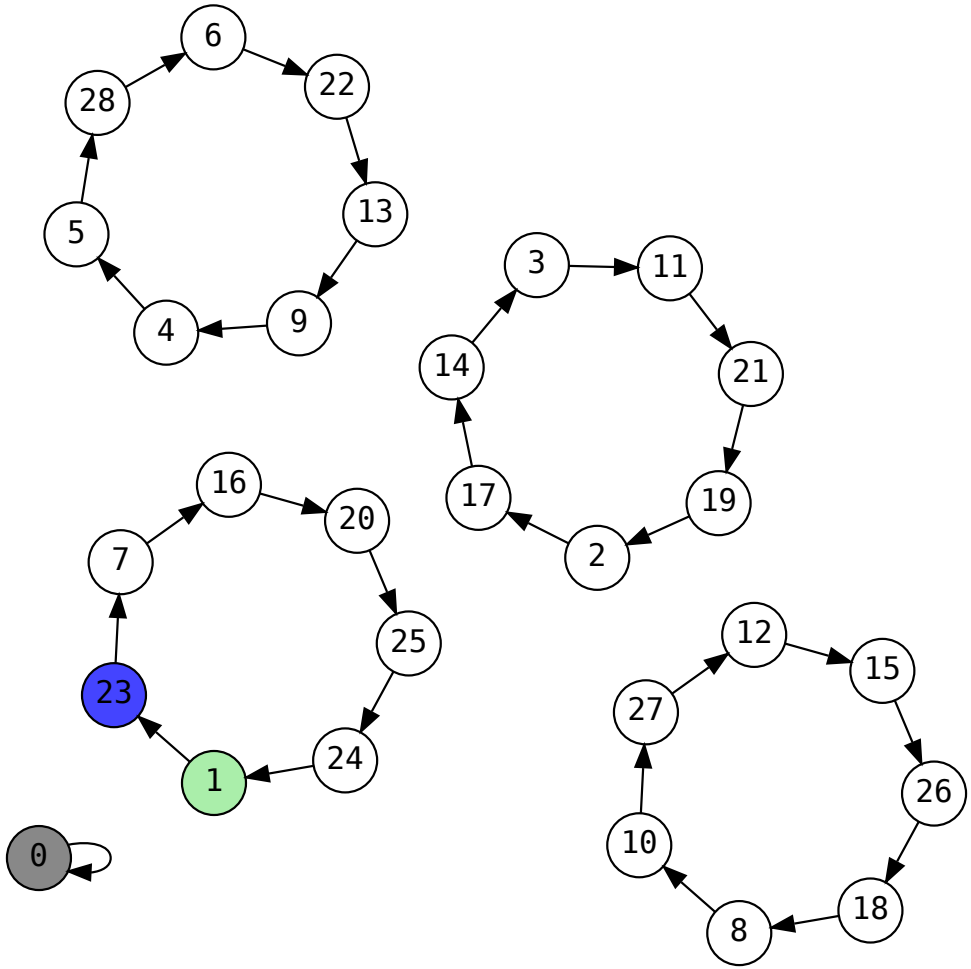
Multiplication, $n = 29, b = 21$



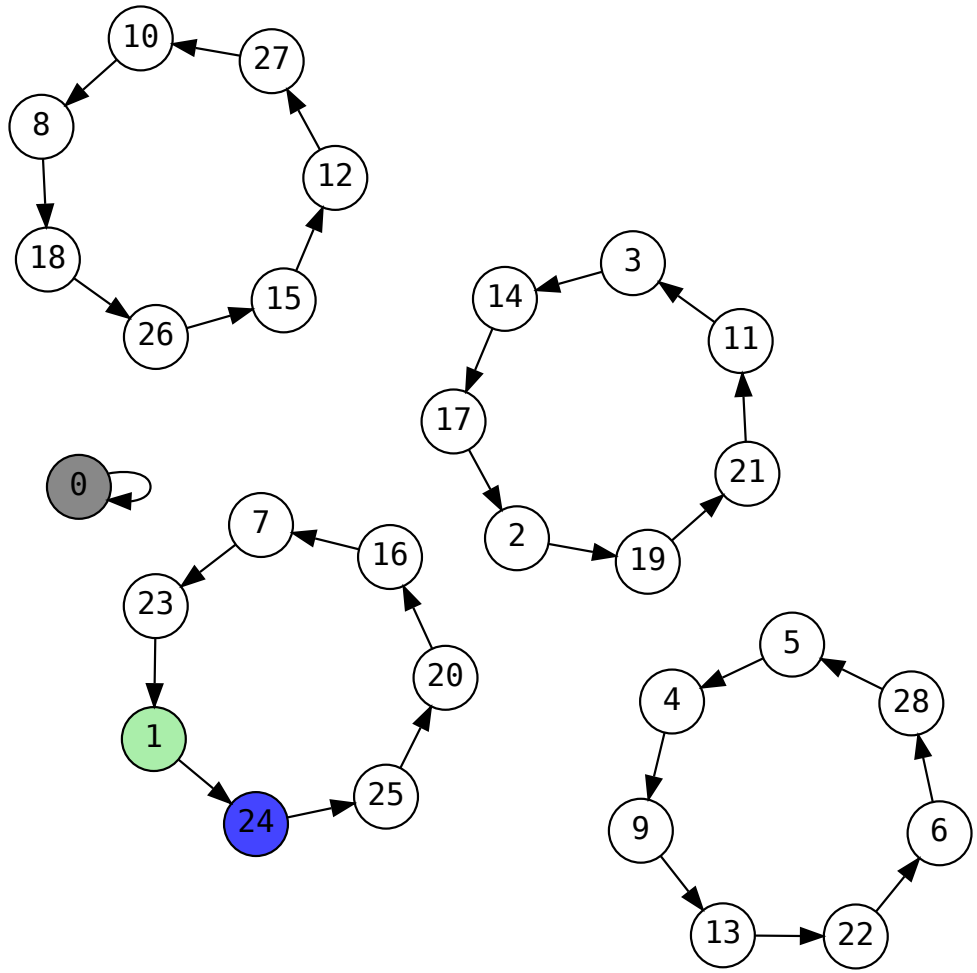
Multiplication, $n = 29, b = 22$



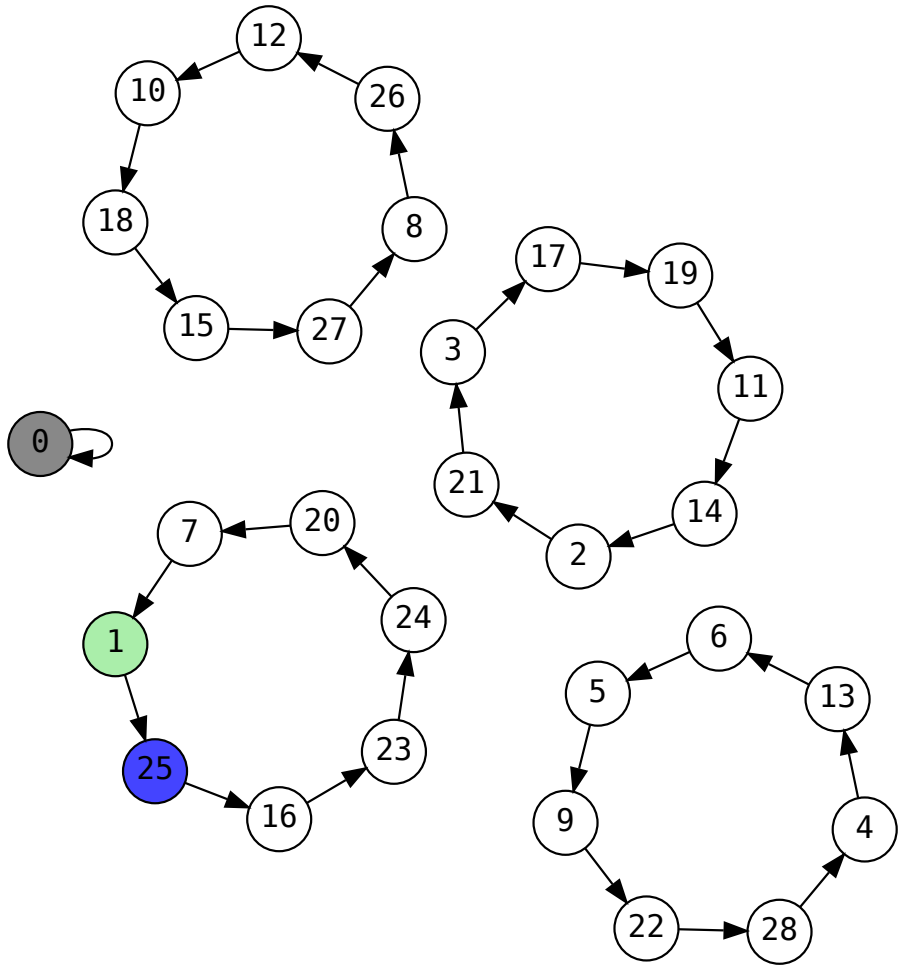
Multiplication, $n = 29, b = 23$



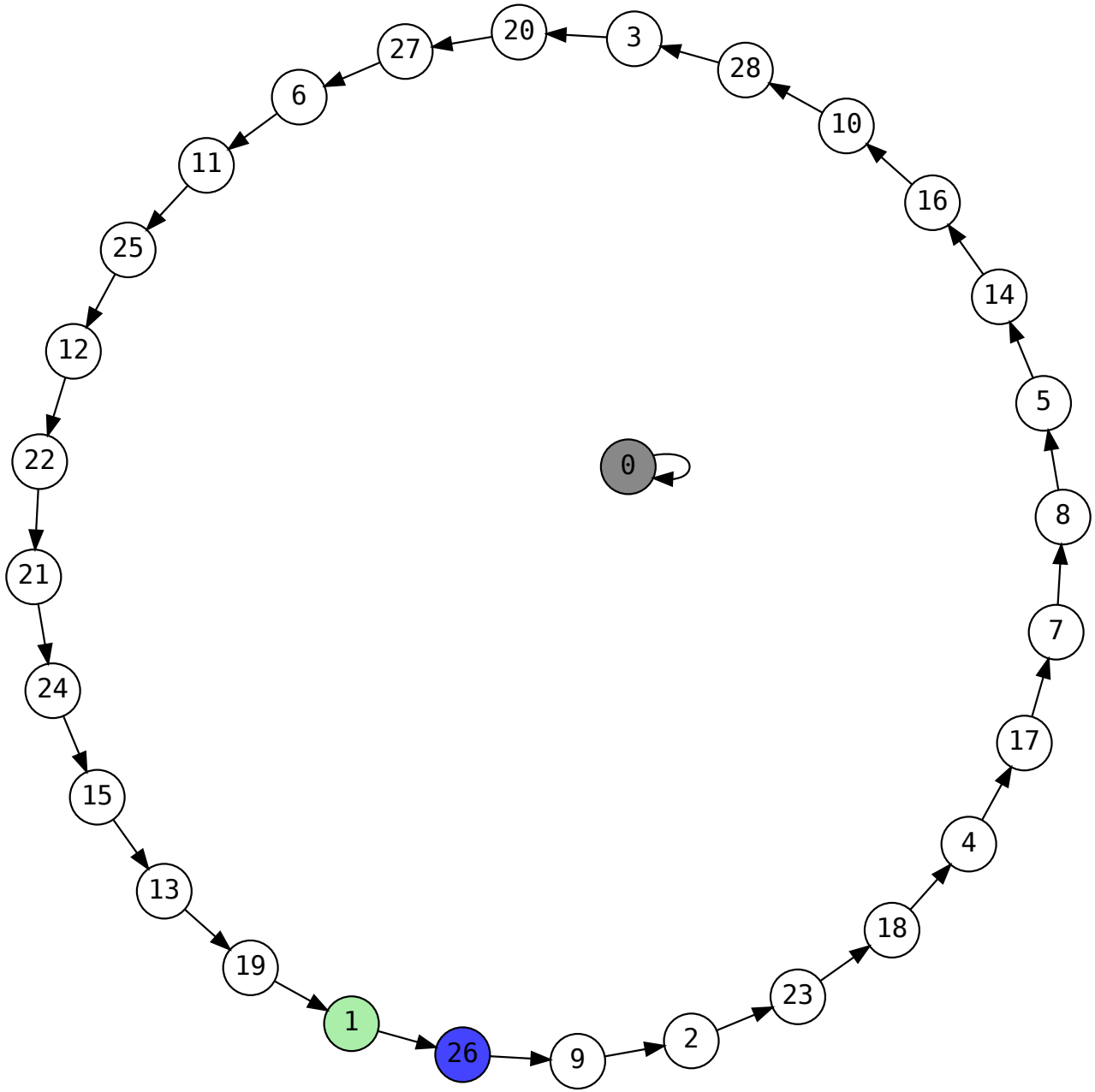
Multiplication, $n = 29, b = 24$



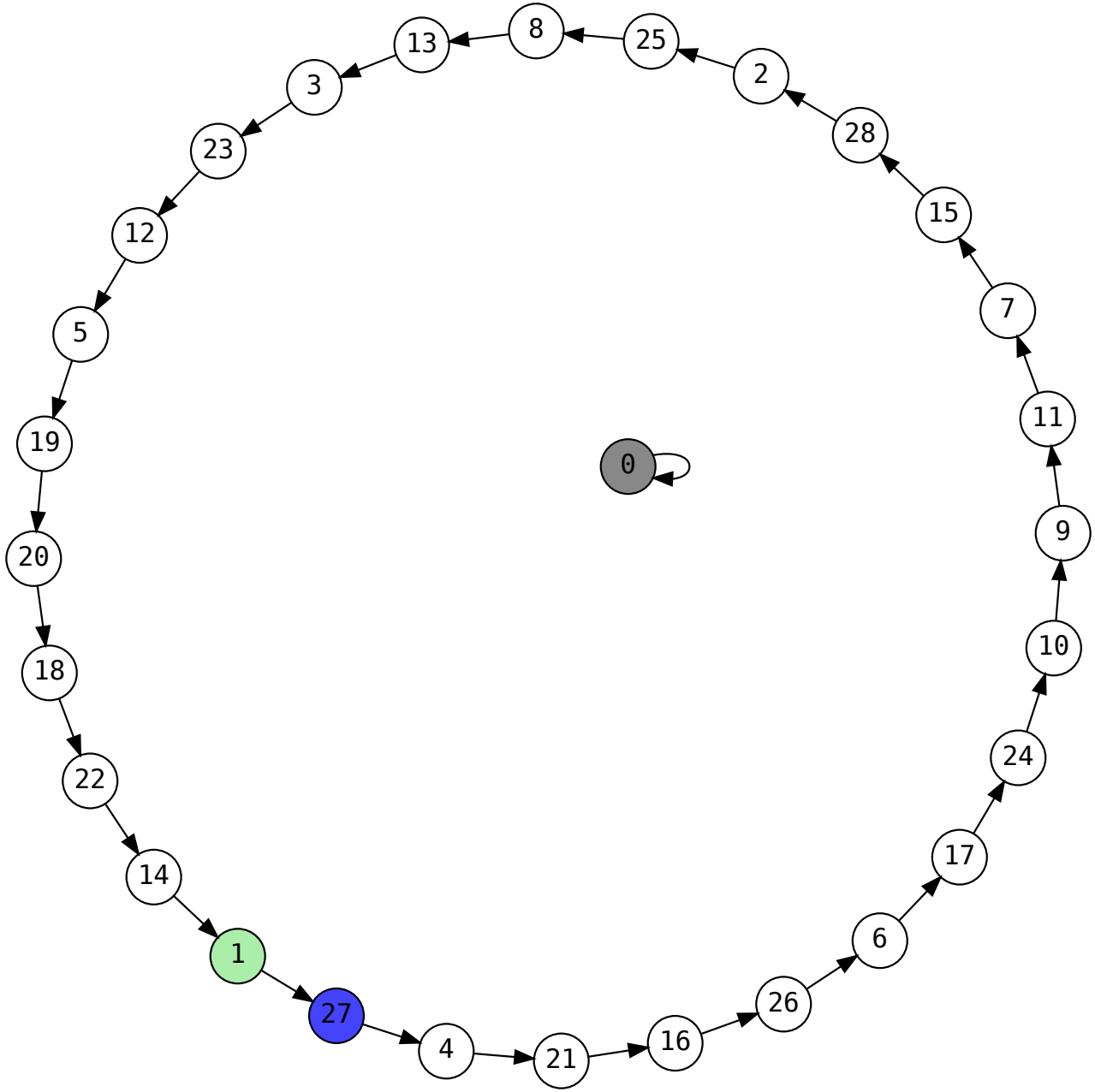
Multiplication, $n = 29, b = 25$



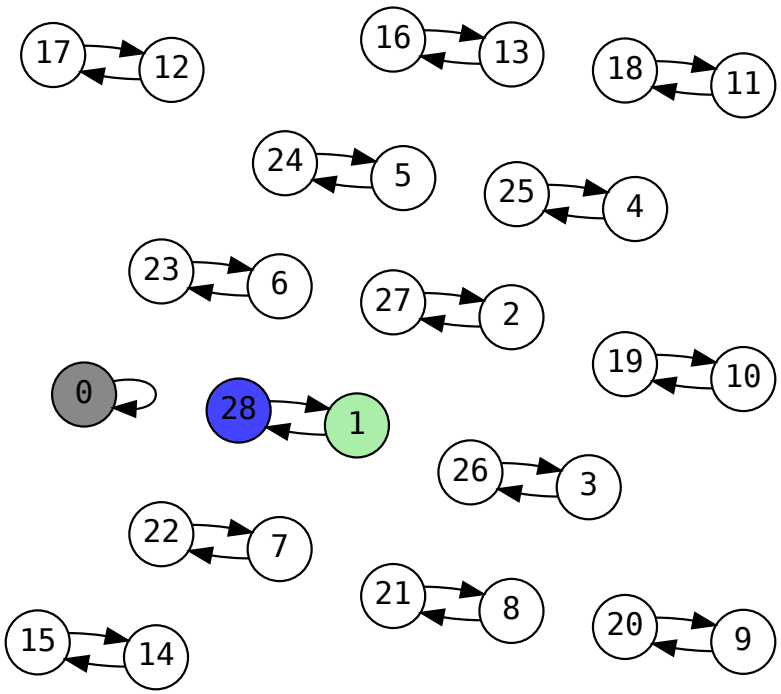
Multiplication, $n = 29, b = 26$



Multiplication, $n = 29, b = 27$

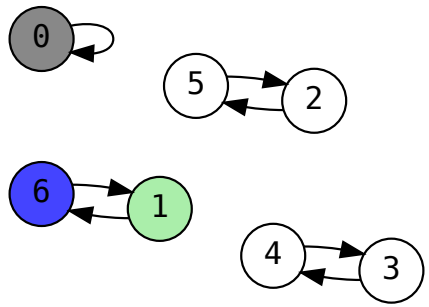


Multiplication, $n = 29, b = 28$

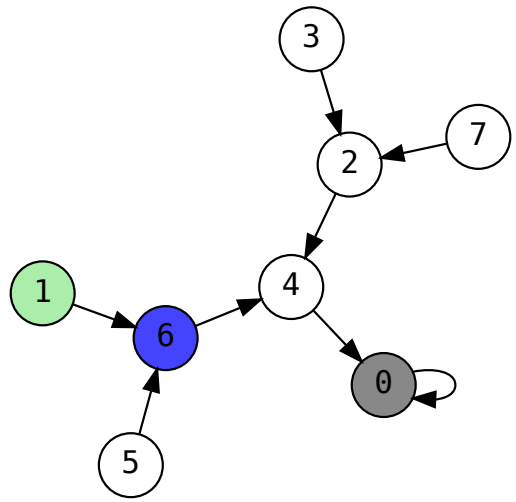


Multiplication, $b = 6$

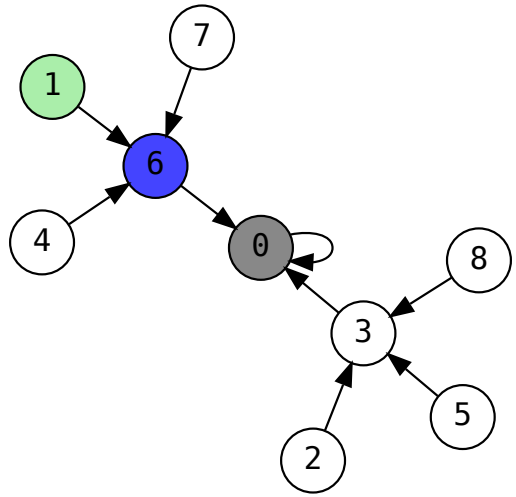
Multiplication, $n = 7, b = 6$



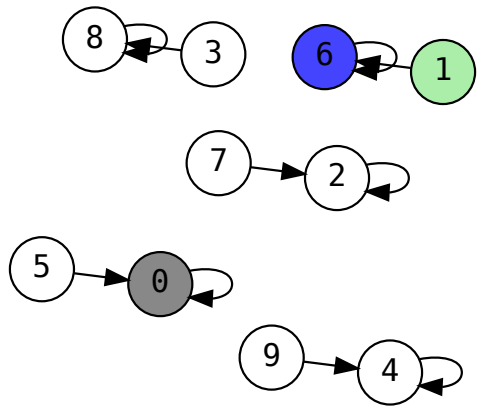
Multiplication, $n = 8, b = 6$



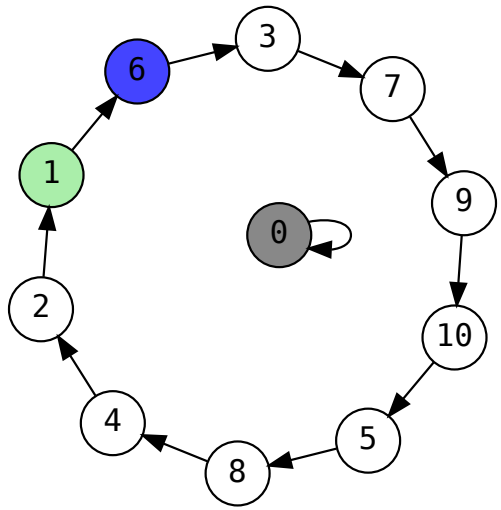
Multiplication, $n = 9, b = 6$



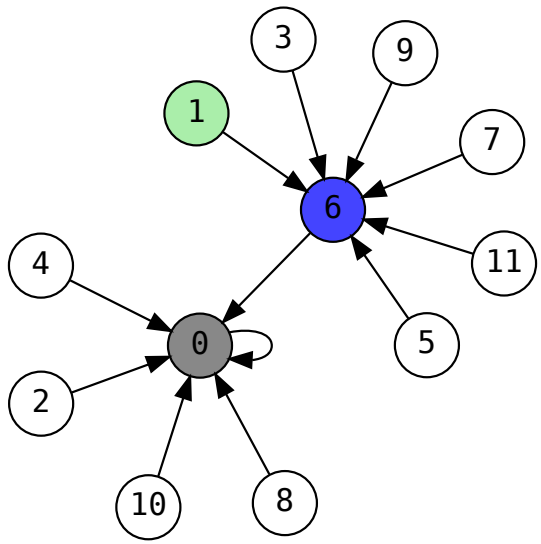
Multiplication, $n = 10, b = 6$



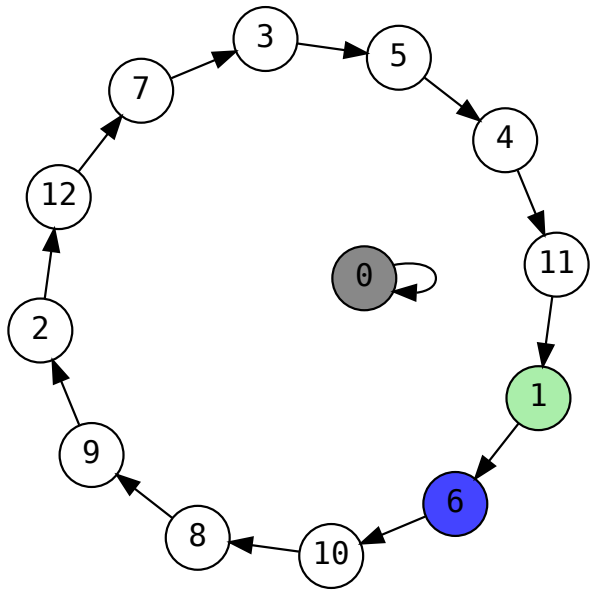
Multiplication, $n = 11, b = 6$



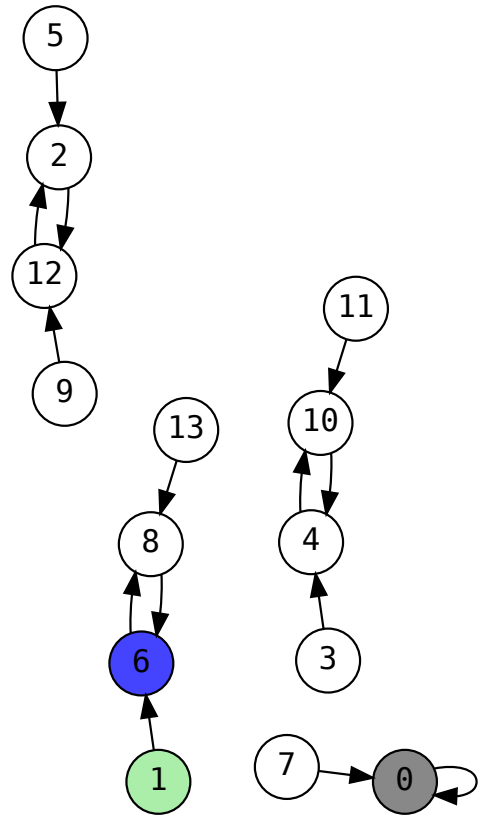
Multiplication, $n = 12, b = 6$



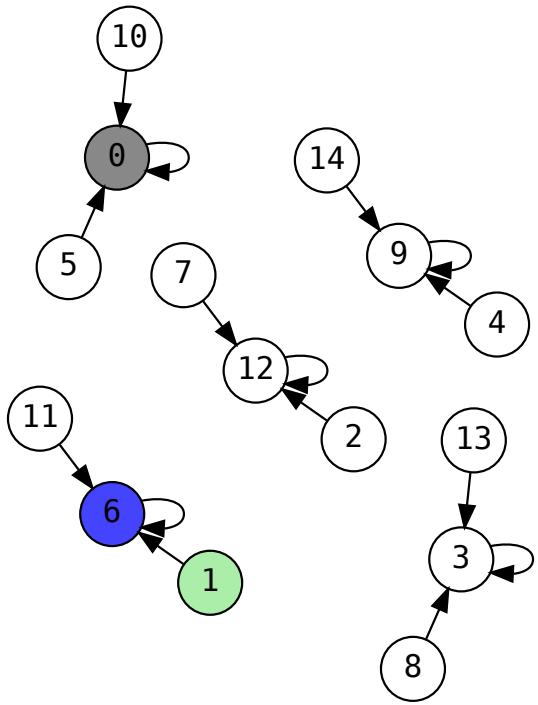
Multiplication, $n = 13, b = 6$



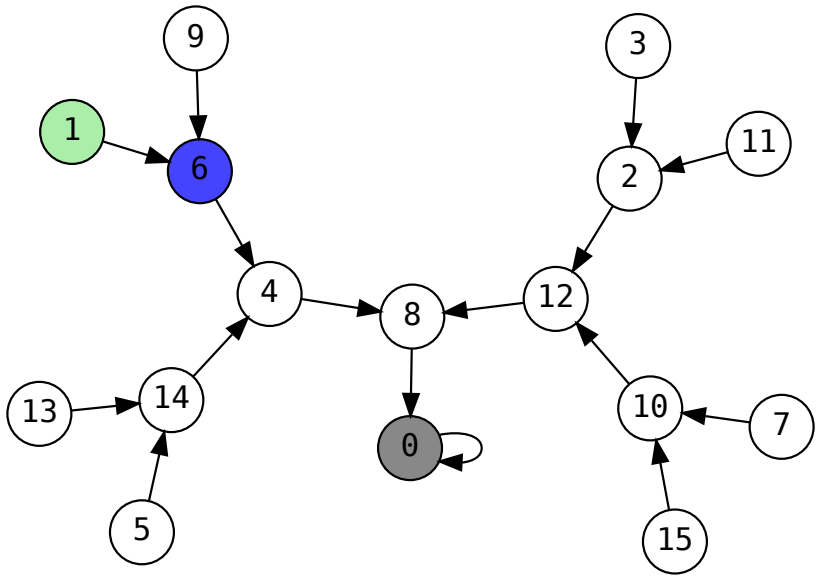
Multiplication, $n = 14, b = 6$



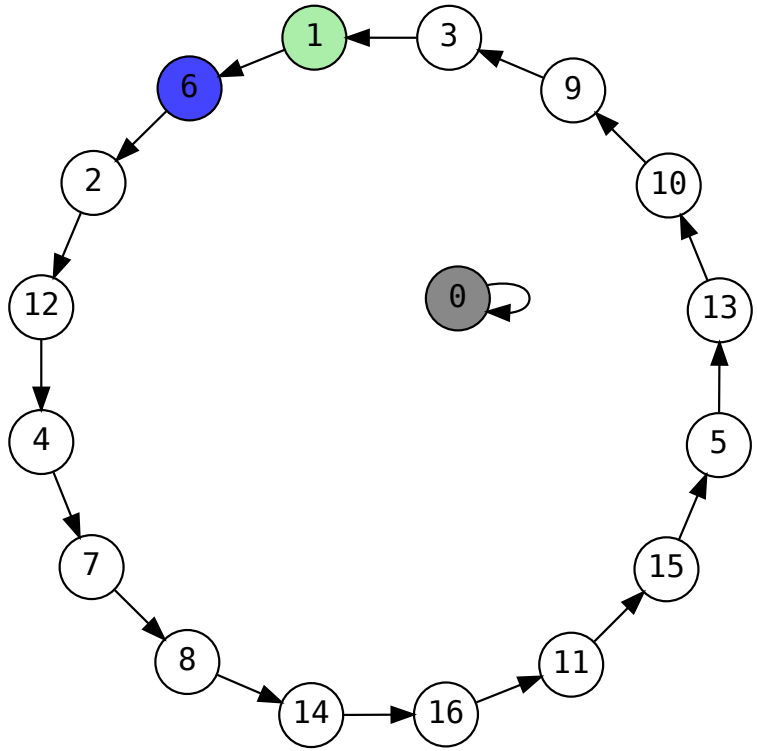
Multiplication, $n = 15, b = 6$



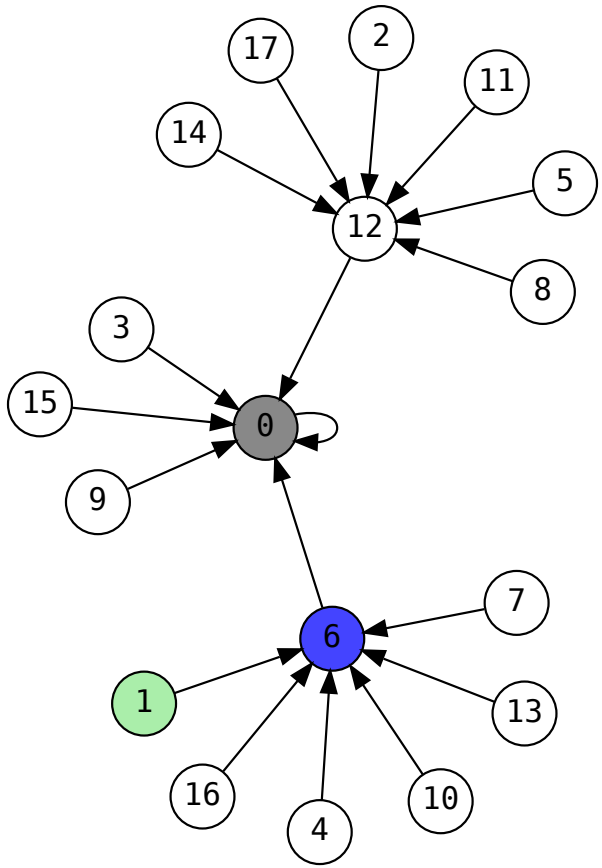
Multiplication, $n = 16, b = 6$



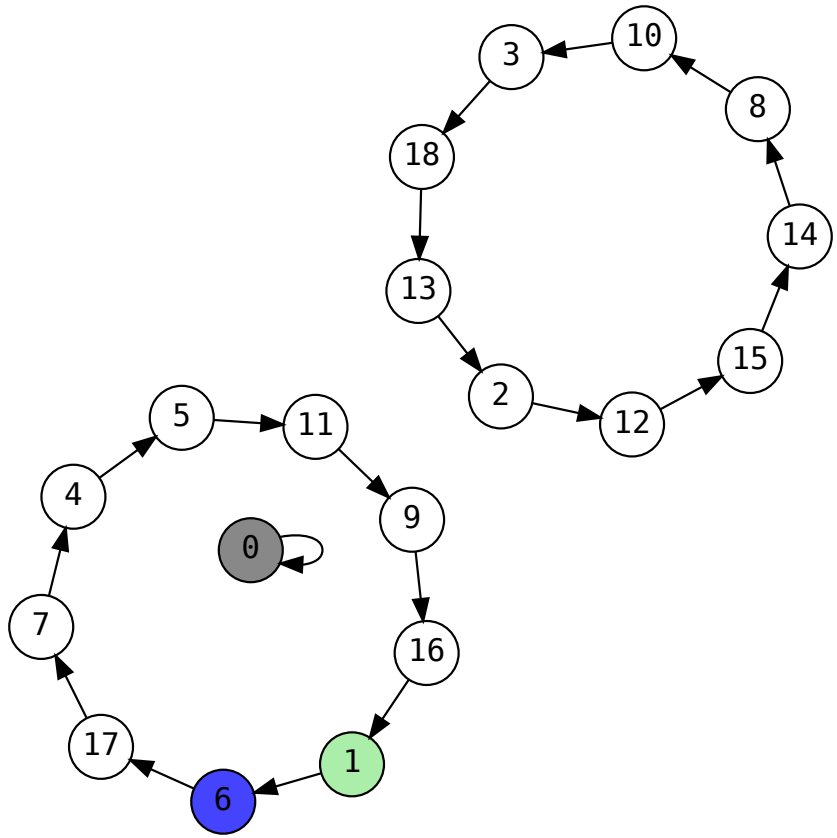
Multiplication, $n = 17, b = 6$



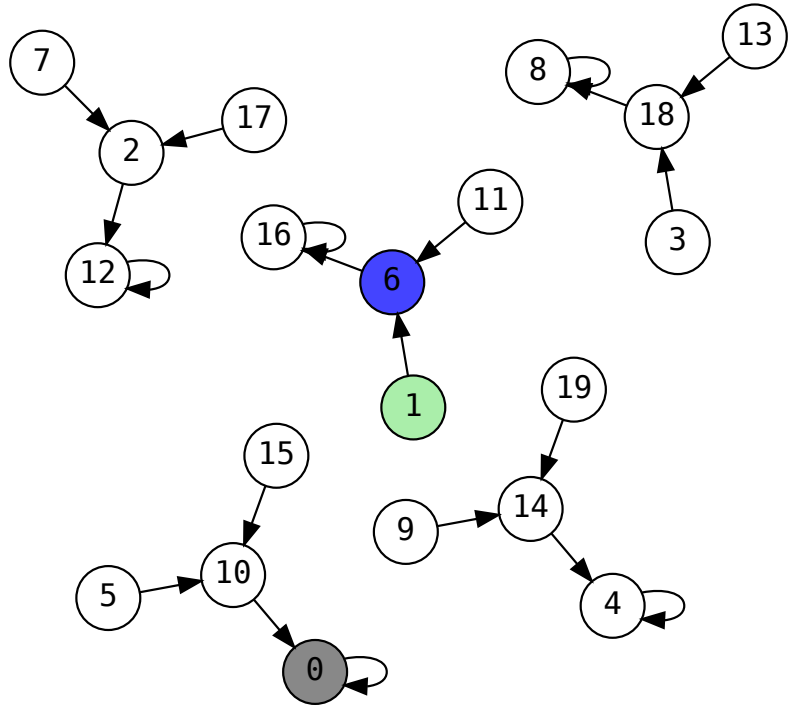
Multiplication, $n = 18, b = 6$



Multiplication, $n = 19, b = 6$



Multiplication, $n = 20, b = 6$



Multiplication mod 10

Subscript indicates $\gcd(x, 10)$.

	0_{10}	1_1	2_2	3_1	4_2	5_5	6_2	7_1	8_2	9_1
0_{10}	0_{10}	0_{10}	0_{10}	0_{10}	0_{10}	0_{10}	0_{10}	0_{10}	0_{10}	0_{10}
1_1	0_{10}	1_1	2_2	3_1	4_2	5_5	6_2	7_1	8_2	9_1
2_2	0_{10}	2_2	4_2	6_2	8_2	0_{10}	2_2	4_2	6_2	8_2
3_1	0_{10}	3_1	6_2	9_1	2_2	5_5	8_2	1_1	4_2	7_1
4_2	0_{10}	4_2	8_2	2_2	6_2	0_{10}	4_2	8_2	2_2	6_2
5_5	0_{10}	5_5	0_{10}	5_5	0_{10}	5_5	0_{10}	5_5	0_{10}	5_5
6_2	0_{10}	6_2	2_2	8_2	4_2	0_{10}	6_2	2_2	8_2	4_2
7_1	0_{10}	7_1	4_2	1_1	8_2	5_5	2_2	9_1	6_2	3_1
8_2	0_{10}	8_2	6_2	4_2	2_2	0_{10}	8_2	6_2	4_2	2_2
9_1	0_{10}	9_1	8_2	7_1	6_2	5_5	4_2	3_1	2_2	1_1

Multiplication mod 10, coprime only

	1_1	3_1	7_1	9_1
1_1	1_1	3_1	7_1	9_1
3_1	3_1	9_1	1_1	7_1
7_1	7_1	1_1	9_1	3_1
9_1	9_1	7_1	3_1	1_1

Multiplication mod 11

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Key Theorem

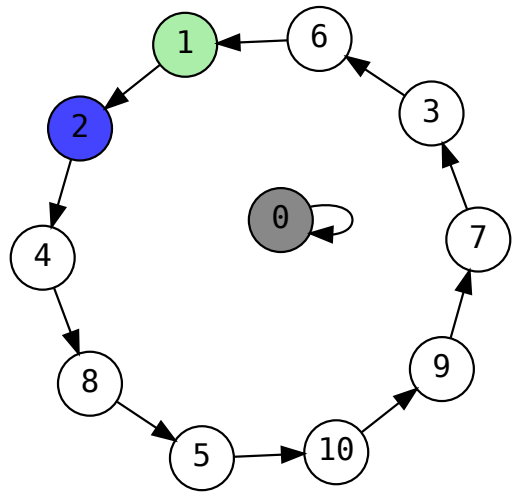
The set of integers $0 < b < n$ where b and n are coprime form a group under multiplication mod n.

n	E_n	$\phi(n)$
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4
11	1,2,3,4,5,6,7,8,9,10	10
12	1,5,7,11	4

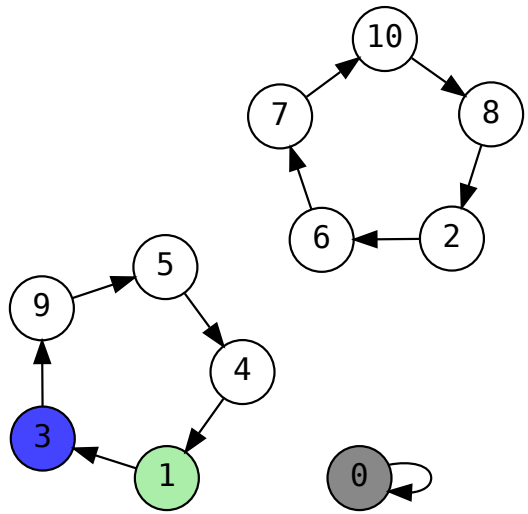
Possibilities

primality of n	$b^{n-1} \equiv 1$	Comment	Example
prime	true	one cycle	11,2
prime	true	multiple cycles	11,3
composite	true	non-witness	9,8
composite	false	witness with 1-cycle	10,3
composite	false	witness with 1-free-cycle	10,2
composite	false	witness without cycle	12,2

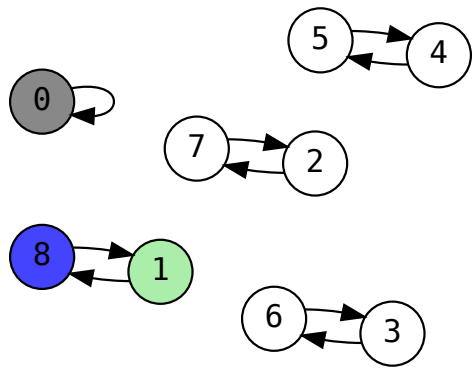
Multiplication, $n = 11, b = 2$



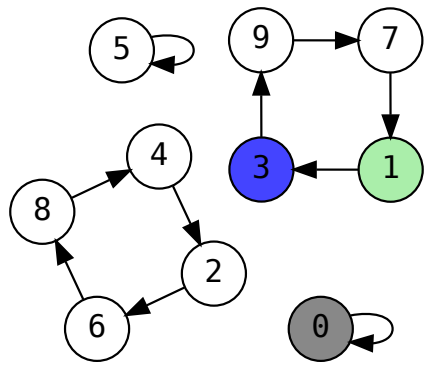
Multiplication, $n = 11, b = 3$



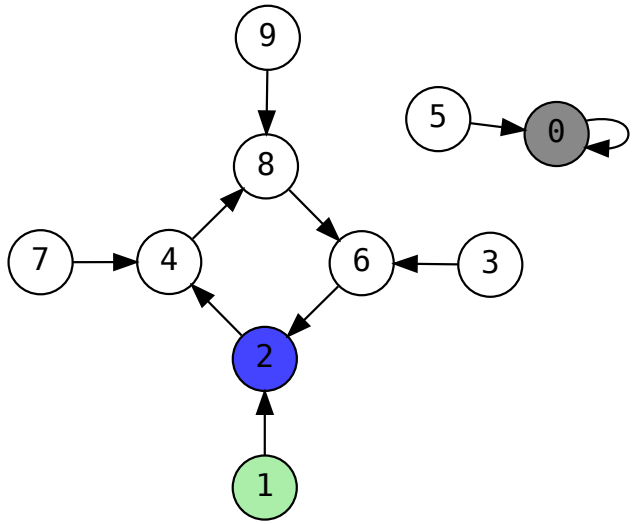
Multiplication, $n = 9, b = 8$



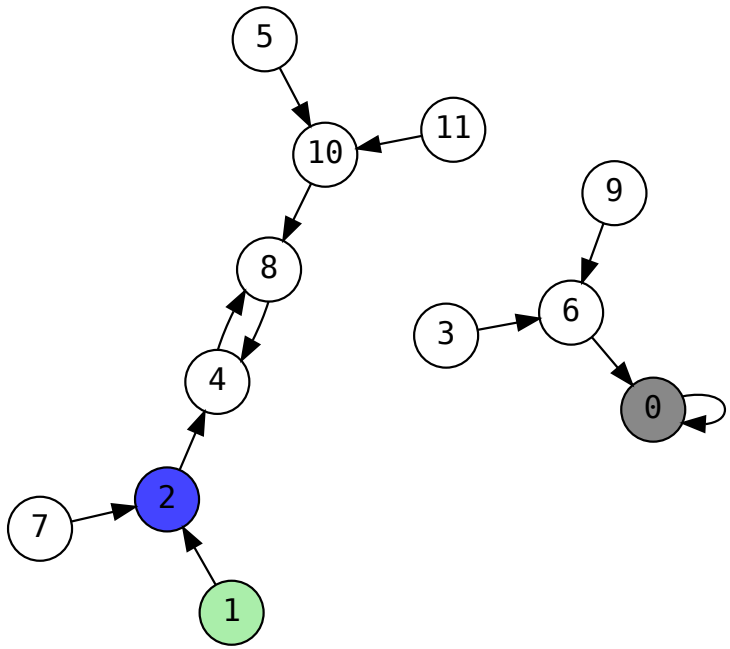
Multiplication, $n = 10, b = 3$



Multiplication, $n = 10, b = 2$



Multiplication, $n = 12, b = 2$



```
witness-b?
```

witness-b?

```clojure
(defn oddify
  "Returns [odd-num two-pow] such that
  n = odd-num * 2^two-pow"
  [n]) ;; impl omitted for brevity

(defn witness-b?
  "Returns true if b produces a
  non-trivial square root of 1."
  [n b]
  (let [[odd-num two-pow] (oddify (dec n))]
    (->> (iterate #(mod (* % %) n)
                  (pow-mod b odd-num n))
         (take (inc two-pow))
         (partition 2 1)
         (some (fn [[x x-squared]]
                 (and (= 1 x-squared)
                      (< 1 x (dec n))))))))
```

$\sqrt{1}$

When p is prime, ± 1 are the only two square roots of $1 \mod p$.

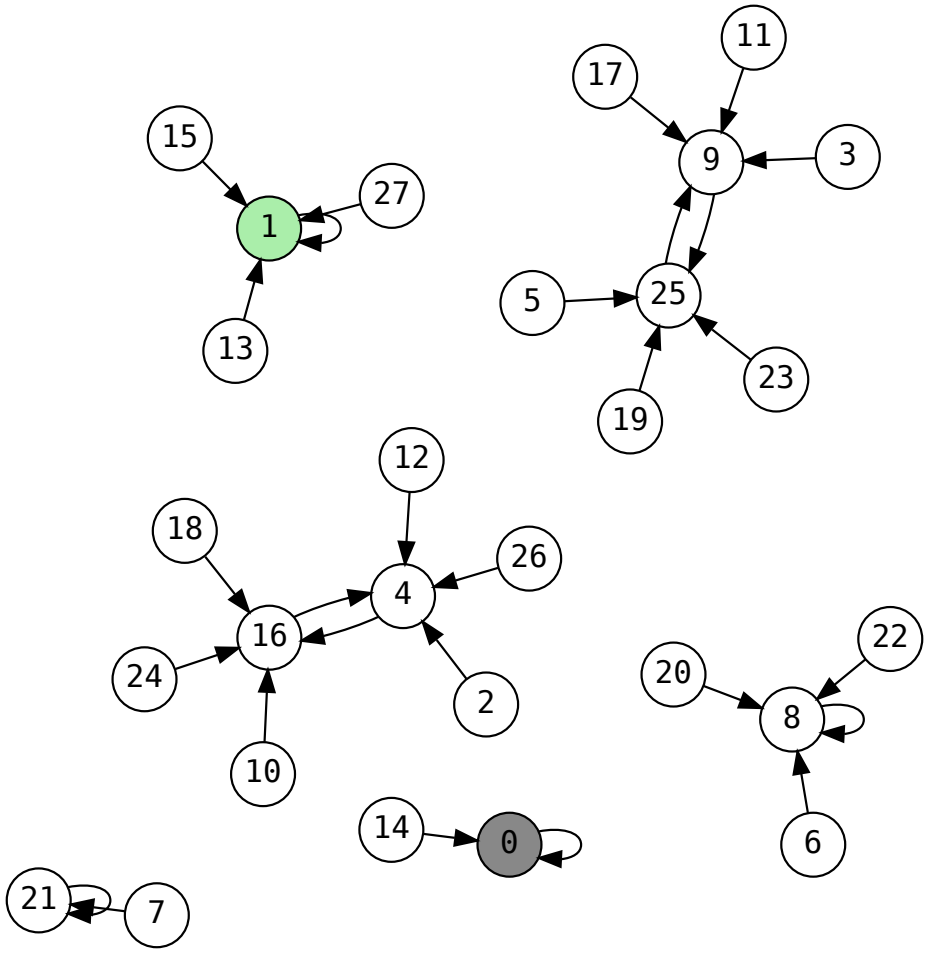
Multiplication mod 11

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

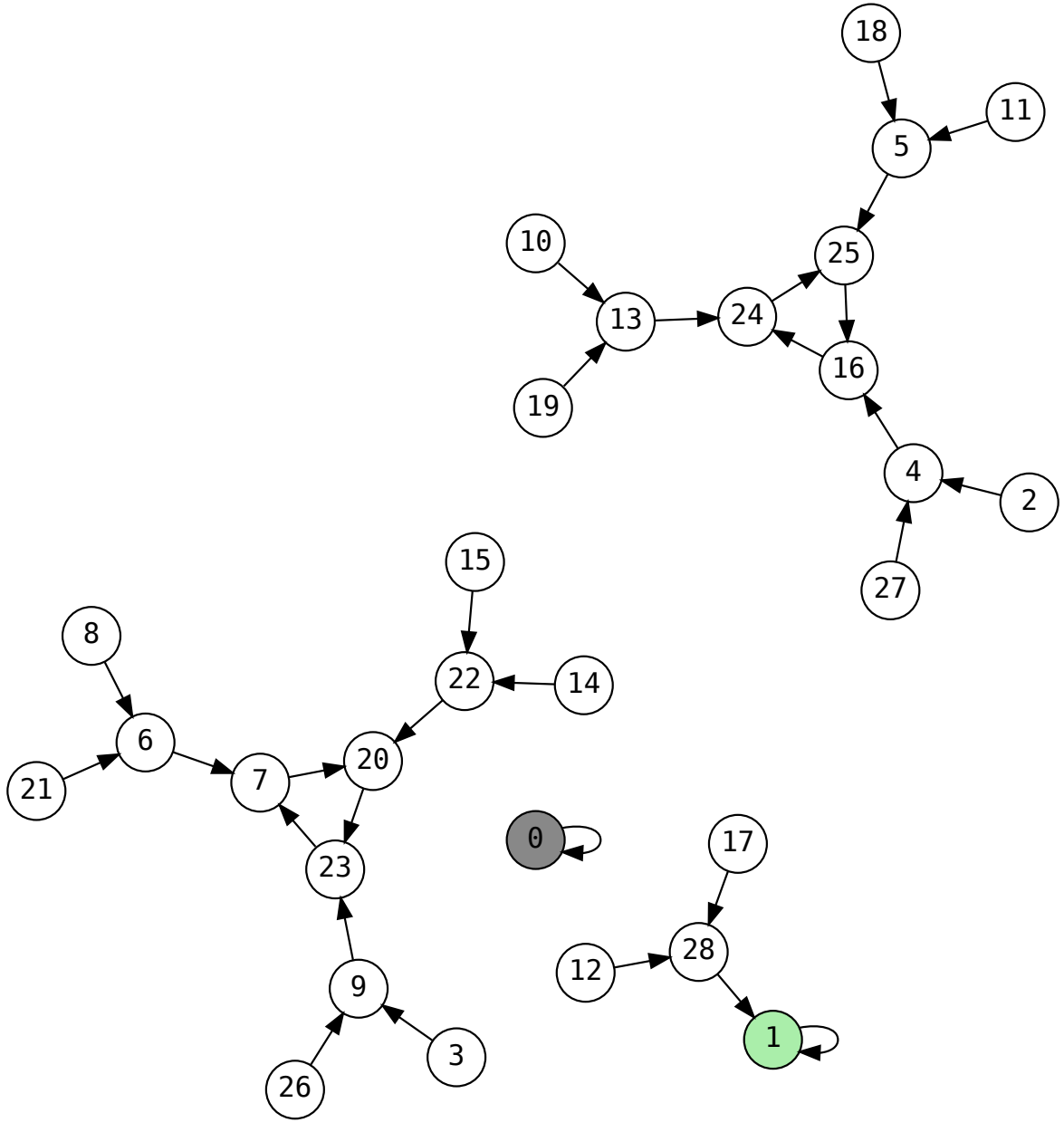
Multiplication mod 8

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Squaring, $n = 28$



Squaring, $n = 29$



$\sqrt{1}$ Count

- 3: 2
- 4: 2
- 5: 2
- 6: 2
- 7: 2
- 8: 4
- 9: 2
- 10: 2
- 11: 2
- 12: 4
- 13: 2
- 14: 2
- 15: 4
- 16: 4
- 17: 2
- 18: 2
- 19: 2
- 20: 4
- 21: 4
- 22: 2
- 23: 2
- 24: 8
- 25: 2
- 26: 2
- 27: 2
- 28: 4
- 29: 2
- 30: 4
- 31: 2
- 32: 4
- 33: 4
- 34: 2
- 35: 4
- 36: 4
- 37: 2
- 38: 2
- 39: 4
- 40: 8
- 41: 2
- 42: 4
- 43: 2
- 44: 4
- 45: 4
- 46: 2
- 47: 2
- 48: 8
- 49: 2
- 50: 2

Why does p have only 2 square roots of 1?

When p is prime, ± 1 are the only two square roots of $1 \mod p$.
Suppose $0 < x < p$ and $x^2 \equiv 1 \mod p$.

Then $x^2 - 1 \equiv 0 \mod p$

and $(x-1)(x+1) \equiv 0 \mod p$

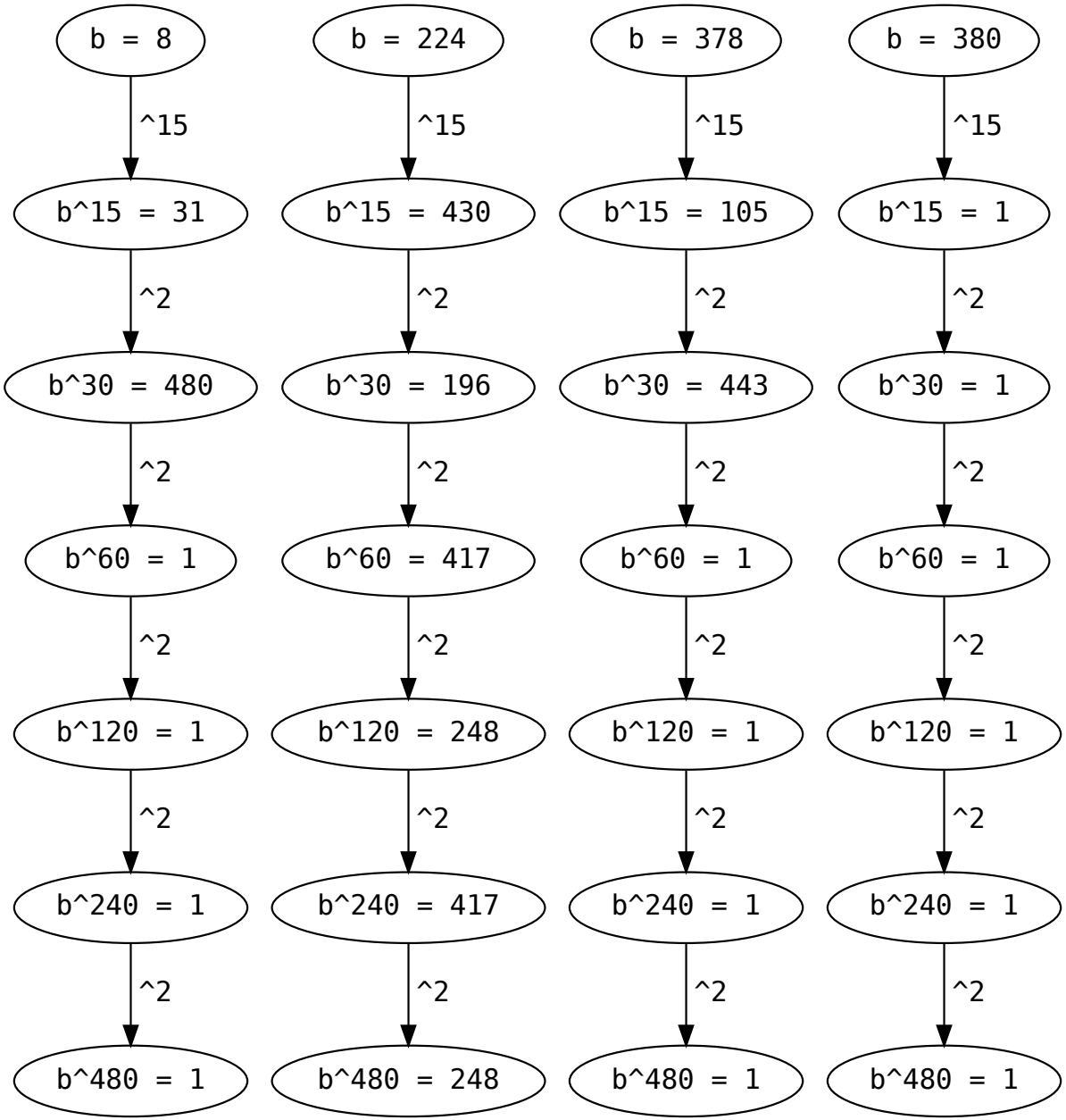
So $(x-1)(x+1)$ is divisible by p, which means at least one of $x-1$ or $x+1$ is divisible by p.

Since $0 < x < p$ it can only be that $x = 1$ or $x = p-1$.

How does b help us find $\sqrt{1}$?

- Square roots mod n are not easy to compute in general, but...
- We know that $b^{n-1} \equiv 1 \mod n$ (because `witness-a?` failed)
- Since $n-1$ is even, we can find $\sqrt{b^{n-1}}$ by computing $b^{\frac{n-1}{2}}$
- If $b^{\frac{n-1}{2}} \equiv 1$ and $\frac{n-1}{2}$ is even, we can find $\sqrt{b^{\frac{n-1}{2}}}$ by computing $b^{\frac{n-1}{4}}$
- ... and so on

Searching for $\sqrt{1}$ with $n = 481 = 1 + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

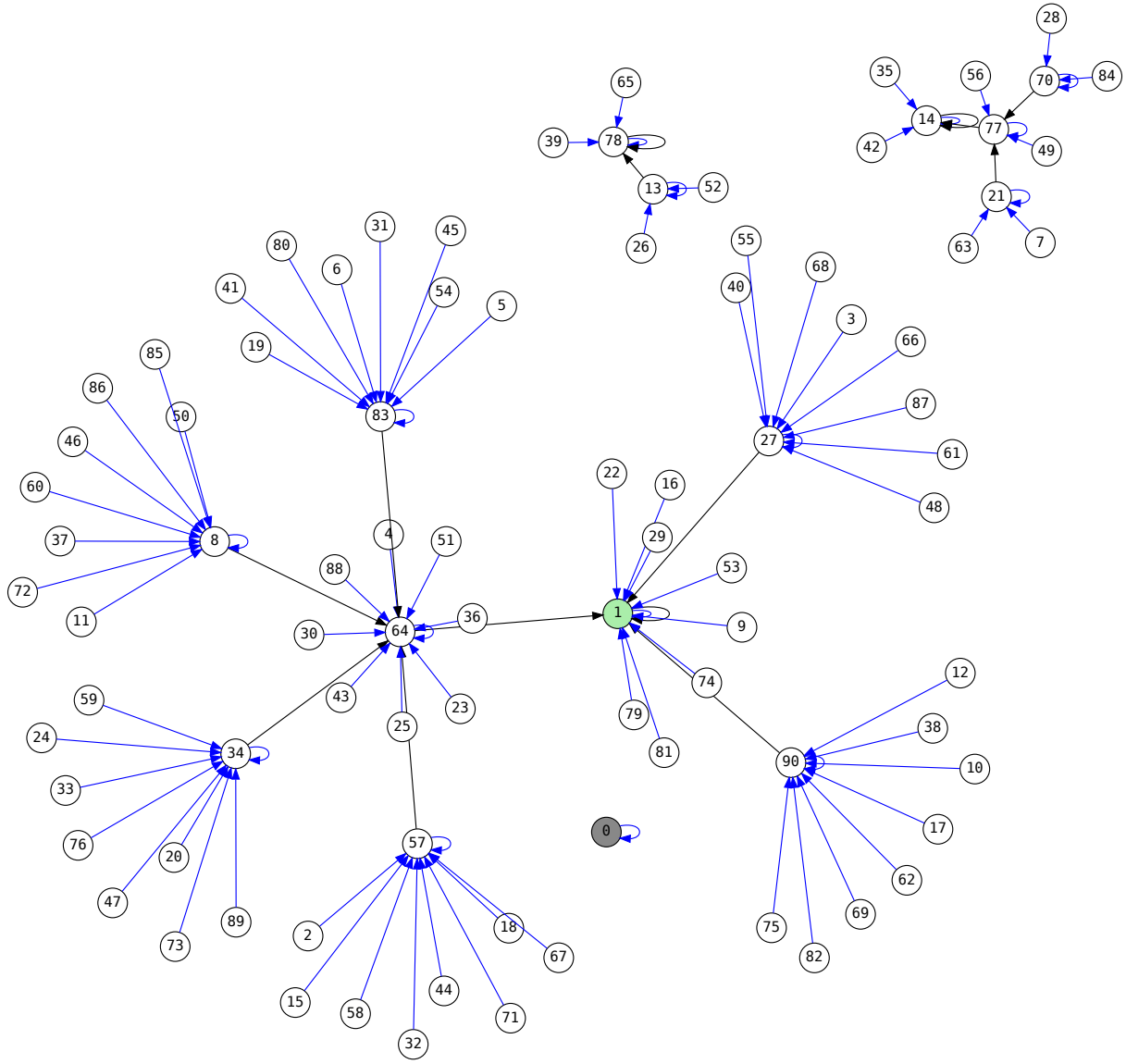


witness-b?

```clojure
(defn oddify
  "Returns [odd-num two-pow] such that
  n = odd-num * 2^two-pow"
  [n]) ;; impl omitted for brevity

(defn witness-b?
  "Returns true if b produces a
  non-trivial square root of 1."
  [n b]
  (let [[odd-num two-pow] (oddify (dec n))]
    (->> (iterate #(mod (* % %) n)
                  (pow-mod b odd-num n))
         (take (inc two-pow))
         (partition 2 1)
         (some (fn [[x x-squared]]
                 (and (= 1 x-squared)
                      (< 1 x (dec n))))))))
```

$\sqrt{1}$-hunting, $n = 91$



$\sqrt{1}$ Count

```clojure
(->> (range 3 10000)
     (filter composite?)
     (map (juxt obstinate? count-sqrts-of-1))
     (frequencies))
```

```
;;=> {[false 2] 739,
;;     [false 4] 4167,
;;     [false 8] 2791,
;;     [false 16] 938,
;;     [false 32] 114,
;;     [false 64] 1,
;;     [true 4] 12,
;;     [true 8] 7}
```

Misc

Performance

Running with `test-count = 100`:

Prime Size (in bits)	Runtime
500	0.19s
1000	1.29s
1500	4.01s
2000	9.11s
2500	17.13s
3000	28.42s
3500	44.60s

Euclid–Mullin sequence

2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, 103, 1079990819, 9539, 3143065813, 29, 3847, 89, 19, 577, 223, 139703, 457, 9649, 61, 4357, 87991098722552272708281251793312351581099392851768893748012603709343, 107, 127, 3313, 2274326891085895327549849150757748483866714395682604207544149407807612458 93, 59, 31, 211, ? ...

a_n is the least prime factor of $\left(\prod_{i<n} a_n\right) + 1$:

- $() + 1 = 2$
- $(2) + 1 = 3$
- $(2 \cdot 3) + 1 = 7$
- $(2 \cdot 3 \cdot 7) + 1 = 43$
- $(2 \cdot 3 \cdot 7 \cdot 43) + 1 = 1807 = (13 \cdot 139)$
- $(2 \cdot 3 \cdot 7 \cdot 43 \cdot 13) + 1 = 23479 = (53 \cdot 443)$
- $(2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 \cdot 53) + 1 = 248867 = (5 \cdot 248867)$

Sample Prime

$$
\begin{aligned}
&267474953546065943730586861208883799484445355286777463223110742880477111954414291442232943456136048254684731181\\
&515171685396993137787258573334555859560686642544629299033800967534406379147734870925967197009748353168633253637429616795670766844878097967011730890641795107975961552199\\
&808862915401921612237489070067067266681022803034339137483184839571715524618508176543817374158483049431724254628016970492137956622015419857030166543496434502264995825029\\
&062339131793274735960716153654409124948964331444788864461889152115805675576581564448117325973212004819541612086923284061862875939241229882045110027039025920062726683314\\
&187628219852718842371380764286946337268445763993189846465009884614818494587144495116283588460698019709338726403523636237361412916503813999313102203372852677236225504973
\end{aligned}
$$

Thanks!

This is the last slide.