How To Guide for nt-tools.exe

Ajeesh T Vijayan
MSc Cryptography
London Metropolitan University

January 20, 2024

Introduction

This document describes how to use the command line tool developed as part of the assignments.

How To

1. Double clicking the ".exe" file will open the app. Below is a screen shot of the landing page of the app.
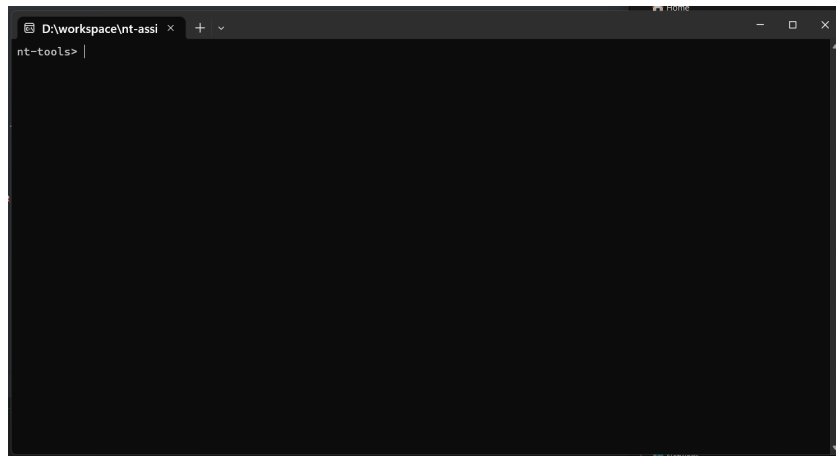

Figure 1: Landing Page

2. Typing "help" or just pressing the "Enter" ⏎ key will display the help.

```
nt-tools> help
NumberTheoryTools:
  primes                     Search for prime numbers between START and END numbers
  composites                 Search for composite numbers between START and END numbers
  composites-pq              Search for composite numbers of the form "p.q" between START and END numbers
  nums-with-primitive-roots  Search for numbers with primitive roots between START and END numbers
  carmichael-nums            Carmichael Number search in a range.
  ifactors                   Finds the Integer Factorisation of a number.
  primality                  Primality checking capabilities.
  miller-rabin-liars         List the Miller-Rabin Liars of a number if any exist
  gcd                        Finds the GCD of two numbers using Euclid's algorithm.
  quadratic-sieve            Integer Factorisation - Quadratic Sieve.
  pollards-p-minus-1         Integer Factorisation - Pollard's P-1 Algm.
  pollards-rho               Pollards Rho Alogorithm to find the logarithm modulo p
  modular-pow                Fast Modular Exponentiation
  aks-findr                  Finds the 'r' value for the AKS algorithm.
  list-primitive-roots       List the primitive roots of a number
  ass2q2b                    Assignment 2 - Question 2b - Primitive Roots - Euler's Totient Function
  ass2q2c                    Assignment 2 - Question 2c - p^k(p > 2, k ≥ 1) or 2p^k(p > 2, k ≥ 1)
  ass2q3d                    Assignment 2 - Question 3d - all numbers of the form n = pq (p and q both odd primes) in your range are included
                               in set B
  aks-failed-steps-for-n     Assignment 1 - Question 4c - Choose any three elements of your set A and calculate the value of r used in the AKS primality
                               test
  clear
  quit
  help                       Print this message or the help of the given subcommand(s)
nt-tools>
```

Figure 2: Help Page

Command Syntax

1. primes

```
primes -s 2800 -e 3100
```

The below screenshot shows a sample output:


```
nt-tools> primes
error: the following required arguments were not provided:
  --start <START>
  --end <END>

Usage: primes --start <START> --end <END>

For more information, try '--help'.
nt-tools> primes -s 2800 -e 3100

Prime Numbers:
```

Number	2851	2909	2969	3037	3089
2801	2857	2917	2971	3041	
2803	2861	2927	2999	3049	
2819	2879	2939	3001	3061	
2833	2887	2953	3011	3067	
2837	2897	2957	3019	3079	
2843	2903	2963	3023	3083	

```
nt-tools>
```

Figure 3: List of prime numbers in a range

2. composites

```
composites --start 2800 --end 3100
```

The below screenshot shows a sample output:

```
D:\workspace\nt-assi  ×   +  ∨
nt-tools> composites
error: the following required arguments were not provided:
  --start <START>
  --end <END>

Usage: composites --start <START> --end <END>

For more information, try '--help'.
nt-tools> composites --start 2800 --end 3100

 Prime Numbers:
```

Number	2821	2842	2865	2885	2907	2929	2949	2973	2992	3014	3035	3057	3078	3100
2800	2822	2844	2866	2886	2908	2930	2950	2974	2993	3015	3036	3058	3080	
2802	2823	2845	2867	2888	2910	2931	2951	2975	2994	3016	3038	3059	3081	
2804	2824	2846	2868	2889	2911	2932	2952	2976	2995	3017	3039	3060	3082	
2805	2825	2847	2869	2890	2912	2933	2954	2977	2996	3018	3040	3062	3084	
2806	2826	2848	2870	2891	2913	2934	2955	2978	2997	3020	3042	3063	3085	
2807	2827	2849	2871	2892	2914	2935	2956	2979	2998	3021	3043	3064	3086	
2808	2828	2850	2872	2893	2915	2936	2958	2980	3000	3022	3044	3065	3087	
2809	2829	2852	2873	2894	2916	2937	2959	2981	3002	3024	3045	3066	3088	
2810	2830	2853	2874	2895	2918	2938	2960	2982	3003	3025	3046	3068	3090	
2811	2831	2854	2875	2896	2919	2940	2961	2983	3004	3026	3047	3069	3091	
2812	2832	2855	2876	2898	2920	2941	2962	2984	3005	3027	3048	3070	3092	
2813	2834	2856	2877	2899	2921	2942	2964	2985	3006	3028	3050	3071	3093	
2814	2835	2858	2878	2900	2922	2943	2965	2986	3007	3029	3051	3072	3094	
2815	2836	2859	2880	2901	2923	2944	2966	2987	3008	3030	3052	3073	3095	
2816	2838	2860	2881	2902	2924	2945	2967	2988	3009	3031	3053	3074	3096	
2817	2839	2862	2882	2904	2925	2946	2968	2989	3010	3032	3054	3075	3097	
2818	2840	2863	2883	2905	2926	2947	2970	2990	3012	3033	3055	3076	3098	
2820	2841	2864	2884	2906	2928	2948	2972	2991	3013	3034	3056	3077	3099	

```
nt-tools>
```

Figure 4: List of composite numbers in a range

3. composites-pq

```
composites-pq --start 2800 --end 3100
```

The below screenshot shows a sample output:

```
D:\workspace\nt-assi  ×   +  ∨

nt-tools> composites-pq
error: the following required arguments were not provided:
  --start <START>
  --end <END>

Usage: composites-pq --start <START> --end <END>

For more information, try '--help'.
nt-tools> composites-pq --start 2800 --end 3100

 Composites N = P.Q:
```

Number	2815	2839	2859	2881	2901	2923	2935	2951	2977	2991	3007	3029	3043	3063	3077	3095
2807	2823	2841	2863	2885	2911	2929	2941	2959	2981	2993	3013	3031	3047	3065	3085	3097
2811	2827	2845	2867	2893	2913	2931	2947	2965	2983	2995	3017	3035	3053	3071	3091	3099
2813	2831	2855	2869	2899	2921	2933	2949	2973	2987	3005	3027	3039	3057	3073	3093	

```
nt-tools>
```

Figure 5: List of composite numbers of the form N = P.Q in a range

4. nums-with-primitive-roots

```
        nums-with-primitive-roots --start 600 --end 750
```

The below screenshot shows a sample output:


```
D:\workspace\nt-assi  ×   +  ∨                               −   □   ×

nt-tools> nums-with-primitive-roots
error: the following required arguments were not provided:
  --start <START>
  --end <END>

Usage: nums-with-primitive-roots --start <START> --end <END>

For more information, try '--help'.
nt-tools> nums-with-primitive-roots --start 600 --end 750
{"Numbers With Primitve Roots":["601","607","613","614","617","619","622","625","626","631","634",
"641","643","647","653","659","661","662","673","674","677","683","686","691","694","698","701","7
06","709","718","719","722","727","729","733","734","739","743","746"]}

{"Numbers Without Primitive Roots":["600","602","603","604","605","606","608","609","610","611","6
12","615","616","618","620","621","623","624","627","628","629","630","632","633","635","636","637
","638","639","640","642","644","645","646","648","649","650","651","652","654","655","656","657",
"658","660","663","664","665","666","667","668","669","670","671","672","675","676","678","679","6
80","681","682","684","685","687","688","689","690","692","693","695","696","697","699","700","702
","703","704","705","707","708","710","711","712","713","714","715","716","717","720","721","723",
"724","725","726","728","730","731","732","735","736","737","738","740","741","742","744","745","7
47","748","749","750"]}
nt-tools>
```

Figure 6: List of numbers with primitive roots in a range

5. carmichael-nums

```
        # Carmichael Numbers using FLT
        1. carmichael-nums --method fermat --start 2800 --end 3100

        # Carmichael Numbers using Korselt criteria
        2. carmichael-nums --method korselt --start 2800 --end 3100
```

The below screenshot shows a sample output:

4

Figure 7: Carmichael Numbers in a range

6. ifactors

```
        # Integer Factorisation of a single number using trial and error
        1. ifactors --num1 2452

        # Integer factorisation of a range of numbers
        2. ifactors --num1 2800 --num2 2850
```

The below screenshot shows a sample output:

Prime Factorisation - Only Composites In The Range:

Number	Factorisation	2813	29^1 x 97^1	2825	5^2 x 113^1	2838	2^1 x 3^1 x 11^1 x 43^1	2850	2^1 x 3^1 x 5^2 x 19^1
2800	2^4 x 5^2 x 7^1	2814	2^1 x 3^1 x 7^1 x 67^1	2826	2^1 x 3^2 x 157^1	2839	17^1 x 167^1		
2802	2^1 x 3^1 x 467^1	2815	5^1 x 563^1	2827	11^1 x 257^1	2840	2^3 x 5^1 x 71^1		
2804	2^2 x 701^1	2816	2^8 x 11^1	2828	2^2 x 7^1 x 101^1	2841	3^1 x 947^1		
2805	3^1 x 5^1 x 11^1 x 17^1	2817	3^2 x 313^1	2829	3^1 x 23^1 x 41^1	2842	2^1 x 7^2 x 29^1		
2806	2^1 x 23^1 x 61^1	2818	2^1 x 1409^1	2830	2^1 x 5^1 x 283^1	2844	2^2 x 3^2 x 79^1		
2807	7^1 x 401^1	2820	2^2 x 3^1 x 5^1 x 47^1	2831	19^1 x 149^1	2845	5^1 x 569^1		
2808	2^3 x 3^3 x 13^1	2821	7^1 x 13^1 x 31^1	2832	2^4 x 3^1 x 59^1	2846	2^1 x 1423^1		
2810	2^1 x 5^1 x 281^1	2822	2^1 x 17^1 x 83^1	2834	2^1 x 13^1 x 109^1	2847	3^1 x 13^1 x 73^1		
2811	3^1 x 937^1	2823	3^1 x 941^1	2835	3^4 x 5^1 x 7^1	2848	2^5 x 89^1		
2812	2^2 x 19^1 x 37^1	2824	2^3 x 353^1	2836	2^2 x 709^1	2849	7^1 x 11^1 x 37^1		

Figure 8: Integer Factorisation

7. primality

```
# Primality check using gcd test
primality --method gcd --num 71

# Primality check using trial division
primality --method trial-division --num 71

# Primality check using Miller Rabin
primality --method miller-rabin --num 71

# Primality check using AKS Algm
primality --method aks --num 71

# Primality check using FLT - Not Implemented
primality --method fermat --num 71
```
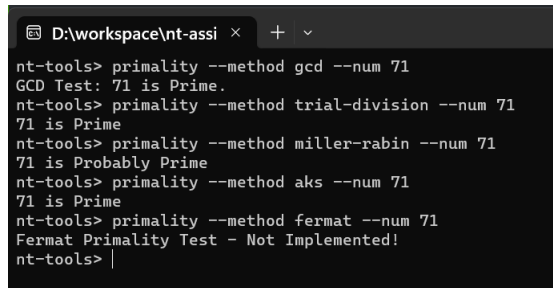
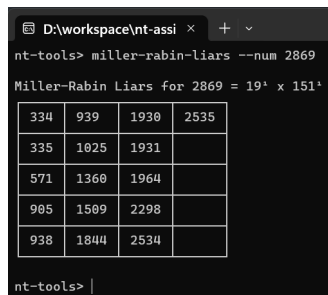The below screenshot shows a sample output:

Figure 9: List of prime numbers in a range

8. miller-rabin-liars

```
miller-rabin-liars --num 2869
```

The below screenshot shows a sample output:

Figure 10: Find the Miller-Rabin Liars of a number

9. gcd

```
            gcd --num1 2000 --num2 200
```

The below screenshot shows a sample output:


```
D:\workspace\nt-assi  ×    +   ∨
nt-tools> gcd
error: the following required arguments were not provided:
  --num1 <NUM1>
  --num2 <NUM2>

Usage: gcd --num1 <NUM1> --num2 <NUM2>

For more information, try '--help'.
nt-tools> gcd --num1 3421 --num2 321

gcd(3421, 321) = 1

nt-tools> gcd --num1 2000 --num2 200

gcd(2000, 200) = 200

nt-tools> gcd --num1 2000 --num2 250

gcd(2000, 250) = 250

nt-tools> gcd --num1 2000 --num2 2500

gcd(2000, 2500) = 500

nt-tools> |
```

Figure 11: GCD of two numbers

10. quadratic-sieve

```
            quadratic-sieve --num 391
```

The below screenshot shows a sample output:


```
D:\workspace\nt-assi  ×    +   ∨
nt-tools> quadratic-sieve
error: the following required arguments were not provided:
  --num <NUM>

Usage: quadratic-sieve --num <NUM>

For more information, try '--help'.
nt-tools> quadratic-sieve --num 391
Square Root of 391 = 19
Legendre Symbol is calculated using Euler's criteria:
If n^(p-1)/2 (mod p) = 1, then (n/p) = 1, else (n/p) = -1
The calculated Factor Base is: [2, 5, 13, 19, 31, 37]
  -46   -27  [1, 1, 0, 2, 0, 0, 0]
  -43   -24  [1, 0, 1, 0, 0, 0, 1]
  -40   -21  [1, 1, 2, 0, 0, 0, 0]
  -31   -12  [1, 0, 0, 1, 1, 0, 0]
  -28    -9  [1, 1, 1, 0, 0, 1, 0]
  -10     9  [1, 1, 1, 0, 0, 1, 0]
   -7    12  [1, 0, 0, 1, 1, 0, 0]
    2    21  [0, 1, 2, 0, 0, 0, 0]
    5    24  [0, 0, 1, 0, 0, 0, 1]
    8    27  [0, 1, 0, 2, 0, 0, 0]
  110   129  [0, 1, 4, 1, 0, 0, 0]
nt-tools> |
```

Figure 12: Quadratic Sieve Evaluation Matrix

11. pollards-p-minus-1

```
            pollards-p-minus-1 --num 78719 --base 13
```

The below screenshot shows a sample output:


```
D:\workspace\nt-assi  ×   +  ∨

nt-tools> pollards-p-minus-1
error: the following required arguments were not provided:
  --num <NUM>
  --base <BASE>

Usage: pollards-p-minus-1 --num <NUM> --base <BASE>

For more information, try '--help'.
nt-tools> pollards-p-minus-1 --num 78719 --base 13
        2         169          1
        3       24950          1
        2       71367          1
        5       11678          1
        7       20871          1
        2       46414          1
        3       20087          1
       11        5690          1
       13       39931          1
        2       31416          1
       17       42006          1
       19       39535          1
       23       24356          1
        5        9177          1
        3       73423          1
       29       27180          1
       31       50831          1
        2       75543        353
78719 = 353 x 223
nt-tools> |
```

Figure 13: Pollard's P-1 Factorisation

12. pollards-rho

```
        pollards-rho --primitive-root 21 -b 47 -m 71
```

The below screenshot shows a sample output:

```
 D:\workspace\nt-assi  ×    +  ∨

nt-tools> pollards-rho
error: the following required arguments were not provided:
  --primitive-root <primitive-root>
  -b <b>
  --modulo <modulo>

Usage: pollards-rho --primitive-root <primitive-root> -b <b> --modulo <modulo>

For more information, try '--help'.
nt-tools> pollards-rho --primitive-root 21 -b 47 -m 71
```

i	x1	a1	b1	x2	a2	b2
1	21	1	0	15	2	0
2	15	2	0	2	8	0
3	12	4	0	16	8	2
4	2	8	0	27	10	2
5	23	8	1	44	21	4
6	16	8	2	10	42	10
7	52	9	2	1	43	11
8	27	10	2	15	18	22
9	19	20	4	2	2	18
10	44	21	4	16	2	20
11	9	21	5	27	4	20
12	10	42	10	44	9	40
13	68	43	10	10	18	12
14	1	43	11	1	19	13

```
Solve the congruence equation: 1x ≡ 12 (mod 35)
nt-tools> |
```

Figure 14: Discrete Logarithm - Pollard's Rho

13. modular-pow

```
    modular-pow -b 26 -e 32 -m 53
```

The below screenshot shows a sample output:


```
 D:\workspace\nt-assi  ×    +  ∨

nt-tools> modular-pow -b 26 -e 32 -m 53

26³²(mod 53) = 24

nt-tools> |
```
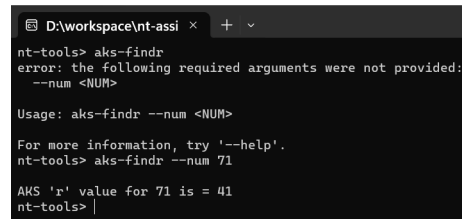
Figure 15: Modular Exponentiation

14. aks-findr

```
        aks-findr --num 71
```

The below screenshot shows a sample output:
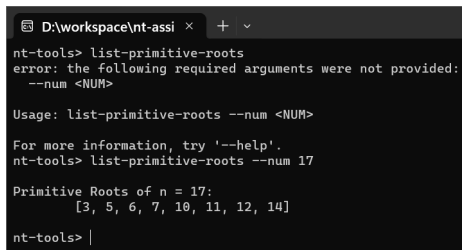
Figure 16: 'r' value of AKS Algm

15. list-primitive-roots

```
        list-primitive-roots --num 17
```

The below screenshot shows a sample output:

Figure 17: List Primitive Roots of a number

16. ass2q2b

```
        ass2q2b --start 50 --end 100
```

The below screenshot shows a sample output:

```
nt-tools> ass2q2b
error: the following required arguments were not provided:
  --start <START>
  --end <END>

Usage: ass2q2b --start <START> --end <END>

For more information, try '--help'.
nt-tools> ass2q2b --start 50 --end 100
```

Prime	φ(p-1)	Prim Roots Count using Trial and Error
53	24	24
59	28	28
61	16	16
67	20	20
71	24	24
73	24	24
79	24	24
83	40	40
89	40	40
97	32	32

```
nt-tools> |
```

Figure 18: Assignment No. 2 Question 2(b) - Number of Primitive Roots

17. ass2q2c

```
ass2q2c --start 50 --end 100
```

The below screenshot shows a sample output:

Figure 19: Number's of the form $p^k, 2p^k$

18. ass2q3d

```
ass2q3d --start 2800 --end 2850
```

The below screenshot shows a sample output:

```
⊟ D:\workspace\nt-assi  ×    +  ∨

nt-tools> ass2q3d --start 2800 --end 2850

Set of numbers without primitive roots:

| 2800 | 2807 | 2813 | 2820 | 2825 | 2830 | 2836 | 2842 | 2849 |
| 2802 | 2808 | 2814 | 2821 | 2826 | 2831 | 2838 | 2844 | 2850 |
| 2804 | 2810 | 2815 | 2822 | 2827 | 2832 | 2839 | 2845 |      |
| 2805 | 2811 | 2816 | 2823 | 2828 | 2834 | 2840 | 2847 |      |
| 2806 | 2812 | 2817 | 2824 | 2829 | 2835 | 2841 | 2848 |      |


Numbers of the form N = P.Q is included in the above table:

| Number | Factorisation | 2845 | 5¹ x 569¹ |
| 2807   | 7¹ x 401¹     |      |           |
| 2811   | 3¹ x 937¹     |      |           |
| 2813   | 29¹ x 97¹     |      |           |
| 2815   | 5¹ x 563¹     |      |           |
| 2823   | 3¹ x 941¹     |      |           |
| 2827   | 11¹ x 257¹    |      |           |
| 2831   | 19¹ x 149¹    |      |           |
| 2839   | 17¹ x 167¹    |      |           |
| 2841   | 3¹ x 947¹     |      |           |

nt-tools> |
```

Figure 20: Primitive Roots & Numbers of form N = P.Q

19. aks-failed-steps-for-n

```
aks-failed-steps-for-n --start 2800 --end 3100
```

The below screenshot shows a sample output:

```
D:\workspace\nt-assi  ×   +  ∨
For more information, try '--help'.
nt-tools> aks-failed-steps-for-n --start 2800 --end 3100

Numbers below failed in step3 of AKS Algm:
```

2800	2824	2847	2870	2892	2915	2938	2961	2984	3006	3030	3053	3075	3098
2802	2825	2848	2871	2893	2918	2940	2962	2985	3007	3031	3054	3076	3099
2804	2826	2849	2872	2894	2919	2941	2964	2986	3008	3032	3055	3077	3100
2805	2827	2850	2873	2895	2920	2942	2965	2987	3009	3033	3056	3078	
2806	2828	2852	2874	2896	2921	2943	2966	2988	3010	3034	3057	3080	
2807	2829	2853	2875	2898	2922	2944	2967	2989	3012	3035	3058	3081	
2808	2830	2854	2876	2899	2923	2945	2968	2990	3013	3036	3059	3082	
2810	2831	2855	2877	2900	2924	2946	2970	2991	3014	3038	3060	3084	
2811	2832	2856	2878	2901	2925	2947	2972	2992	3015	3039	3062	3085	
2812	2834	2858	2880	2902	2926	2948	2973	2993	3016	3040	3063	3086	
2813	2835	2859	2881	2904	2928	2949	2974	2994	3017	3042	3064	3087	
2814	2836	2860	2882	2905	2929	2950	2975	2995	3018	3043	3065	3088	
2815	2838	2862	2883	2906	2930	2951	2976	2996	3020	3044	3066	3090	
2816	2839	2863	2884	2907	2931	2952	2977	2997	3021	3045	3068	3091	
2817	2840	2864	2885	2908	2932	2954	2978	2998	3022	3046	3069	3092	
2818	2841	2865	2886	2910	2933	2955	2979	3000	3024	3047	3070	3093	
2820	2842	2866	2888	2911	2934	2956	2980	3002	3026	3048	3071	3094	
2821	2844	2867	2889	2912	2935	2958	2981	3003	3027	3050	3072	3095	
2822	2845	2868	2890	2913	2936	2959	2982	3004	3028	3051	3073	3096	
2823	2846	2869	2891	2914	2937	2960	2983	3005	3029	3052	3074	3097	

```
Numbers below failed in step1 of AKS Algm:
```

2916
3025

```
nt-tools>
```

Figure 21: List of numbers failed the AKS at each of steps

20. clear or cls

   Clears the screen.

21. quit or exit

14