発表なう #scis2010

返信

7:40 PM Jan 21st from TweetDeck

k4403

4403

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

CSS×2.0デビューしています

SCISでは昼デビューしたことがないのに，夜デビューです．ごめんなさい．KY．

CSS×2.0では一貫して**境界研究**について話しています．今回も理論と実装のギャップ，つまり境界について，おはなしします．返信

k4403

4403

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

今日のおはなし

冬休みにfactoring_bot[*1]という簡単なボットを作りました．夏休みにはARでseco-p[*2]を実装しました．

今日は理論を実装するときに直面する困難についておはなしします．

注※**真面目な話です**

返信

k4403

4403

*1 @factoring_bot，愛称「ふぁくたん」
*2 CSS×2.0 in 2009にて発表

factoring_bot??

2010年1月4日
20時56分

素因数分解botとか面白そうかなと思ってみる。だけど僕には~~ピアノがない、君に聴かせる~~腕もないのでとりあえず人力で、189 = 3 * 3 * 3 * 7、1007 = 19 * 53
RT @xagawa [博論] 189pages. 1007kB也

返信

8:56 PM Jan 4th from web

MarriageTheorem

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

要求仕様

1. つぶやきを素因数分解する

以上

返信

k4403

4403

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

GOLDEN RULES

1. 同じつぶやきを2度しない
   - TLが汚染されるので慎ましく
2. 自分のIDが含まれるつぶやきに反応しない
   - 無限RT対策（最も簡単な手法）

返信

k4403

4403

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

実装開始

ボット用アカウント @factoring_bot ゲットなう！

返信

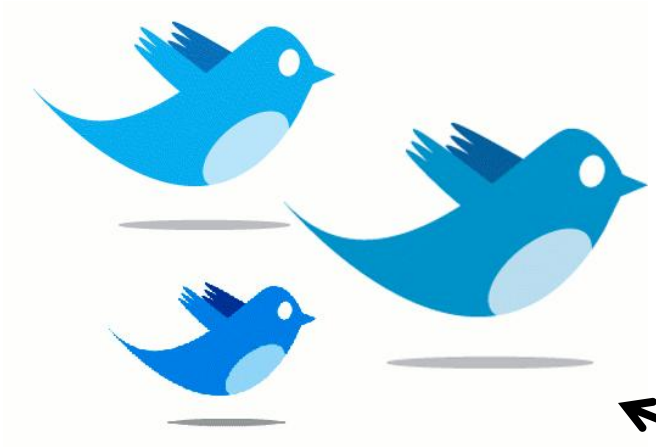
10:08 PM Jan 4th from Echofon

k4403

4403

アルゴリズムとモデル図

Twitter



1. つぶやきの取得

4. RTでつぶやく

2-3. 素因数分解をするなど

アルゴリズム

1. つぶやきの取得
2. つぶやきから素因数分解対象の数字を探す
3. 数字を既知素数表の小さい素数で順番に割っていく
4. 結果をRTでつぶやく

注※開発速度を最優先としてPHPで実装した

理論実装の困難1

該当分野の知識が必要

- **素因数分解に関する知識**
- Twitterに関する知識

そんなことよりも【急募】3桁の数字を素因数分解するために必要な既知素数の上限値. 499この辺？

返信

10:30 PM Jan 4th from Echofon

k4403

4403

一般に、N以下の数を素因数分解するにはsqrt(N)以下の素数を知っていれば充分です。その数が素数でないとしたら、素因数の少なくとも一つはsqrt(N)以下なので。 RT @k4403 そんなことよりも【急募】3桁の数字を素因数分解するために必要な既知素数の上限値．499この辺？

返信

10:36 PM Jan 4th from web

MarriageTheorem

初期化部

```php
<?php
$username = "";
$password = "";
$filename = "";
```

素数表2-9973

```
$fact_nums= array(2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,
101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199,211,223,
227,229,233,239,241,251,257,263,269,271,277,281,283,293,307,311,313,317,331,337,347,349,353,
359,367,373,379,383,389,397,401,409,419,421,431,433,439,443,449,457,461,463,467,479,487,491,
499,503,509,521,523,541,547,557,563,569,571,577,587,593,599,601,607,613,617,619,631,641,643,
647,653,659,661,673,677,683,691,701,709,719,727,733,739,743,751,757,761,769,773,787,797,809,
811,821,823,827,829,839,853,857,859,863,877,881,883,887,907,911,919,929,937,941,947,953,967,
971,977,983,991,997,1009,1013,1019,1021,1031,1033,1039,1049,1051,1061,1063,1069,1087,1091,
1093,1097,1103,1109,1117,1123,1129,1151,1153,1163,1171,1181,1187,1193,1201,1213,1217,1223,
1229,1231,1237,1249,1259,1277,1279,1283,1289,1291,1297,1301,1303,1307,1319,1321,1327,1361,
1367,1373,1381,1399,1409,1423,1427,1429,1433,1439,1447,1451,1453,1459,1471,1481,1483,1487,1489,1493,1499,1511,1523,1531,1543,1549,1553,1559,1567,1571,1579,1583,1597,1601,1607,1609,1613,1619,1621,1627,1637,1657,1663,1667,1669,1693,1697,1699,1709,1721,1723,1733,1741,1747,1753,1759,1777,1783,1787,1789,1801,1
3163,3167,3169,3181,3187,3191,3203,3209,3217,3221,3229,3251,3253,3257,3259,3271,3299,3301,3307,3313,3319,3323,3329,3331,3343,3347,3359,3361,3371,3373,3389,3391,3407,3413,3433,3449,3457,3461,3463,3467,3469,3491,3499,3511,3517,3527,3529,3533,3539,3541,3547,3557,3559,3571,3581,3583,3593,3607,3613,3617,3623,3
```

つぶやきを取得するなど部

```php
$fp = @fopen($filename,'rb') or die("ファイルが開けません");
flock($fp, LOCK_EX);
$line = fgets($fp, 64);
fclose($fp);

$host = "http://twitter.com/statuses/friends_timeline.xml";

if(!empty($line)) {
    $last_id=$line;
    $host .="?since_id=".$last_id;
} else {
    $host .="?count=1";
}

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $host);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
curl_setopt($ch, CURLOPT_USERPWD, "$username:$password");
curl_setopt($ch, CURLOPT_HTTP_VERSION, CURL_HTTP_VERSION_1_1);
$result = curl_exec($ch);
curl_close($ch);
$XML = simplexml_load_string($result);

$i = count($XML)-1;
$j = 0;
while($i >= $j) {
    $var =  $XML->status[$i]->text;
    $reply_name = $XML->status[$i]->user->screen_name;
    $name = $XML->status[$i]->user->name;
```

素因数分解対象数字探索部

```php
    if($reply_name != $username){
        if( !preg_match ( "/@[a-zA-Z0-9-_]{3,}/", $var ) ){
            if( preg_match ( "/([^0-9#]|^)([1-9][0-9]{2,7})([^0-9]|$)/", $var, $matches )){
                $num = $matches[2];
                if($num==2010) break;
```

主要部分
素因数分解してつぶやく部

```php
                $stack = array();
                for($n=0; $n<count($fact_nums); $n++) {
                    if($num <= $fact_nums[$n]) break;
                    if(0 == $num%$fact_nums[$n]) {
                        $num/=$fact_nums[$n];
                        array_push($stack, $fact_nums[$n]);
                        $n--;
                    }
                }
                if(0==count($stack)) {
                    $message = $matches[2].' is prime!';
                } else {
                    $message = $matches[2].'=';
                    foreach($stack as $val) {
                        $message .= $val.'*';
                    }
                    $message .= $num;
                }
                $message .= ' RT @'.$reply_name.': '.$var;
                tweet($message ,$username,$password);
            }
        }
    }
    $i--;
}

if($last_id<$XML->status[0]->id) {
    $last_id = $XML->status[0]->id;
    $dat = (string)$last_id;
    file_put_contents($filename,$dat,LOCK_EX);
}
```

いろいろな後始末部

つぶやき関数

```php
function tweet($message ,$username,$password) {
    $message =urlencode($message);
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, 'http://twitter.com/statuses/update.xml');
    curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 2);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, "status=$message ");
    curl_setopt($ch, CURLOPT_USERPWD, "$username:$password");
    $buffer = curl_exec($ch);
    curl_close($ch);
}

?>
```

理論実装の困難2

20:80ルール適用

- **本質部分は全体の20%**
- 残りの80%は動かすために必要

理論実装の困難3

性能制限

- 素因数分解における性能制限
- **そうじゃない性能制限**

素因数分解できない

[ac] いぢわる.
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
369

返信

12:28 AM Jan 5th from web

Free the SHA-3 rounds parameter

expl01t
exploit

→
とりま3～8桁の数字のみを
素因数分解することに

理論実装の困難4

実用のためのリファイン

- 理論を実装するだけでは使えない
- **実用に耐えるように肉付けが必要**

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

もはや自然言語処理

@k4403 なるほど把握。RTの文字列を本文の文字数によって調整できるといいですね。引用文では数字の前後を省略するとか。

返信

12:50 AM Jan 5th from Echofon in reply to k4403

shokohitsuji

よねしょー

factoring_botの功績の数々

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

はじめてのおしごと
問題提起から3時間後

123=3*41 RT @4403: 123

返信

11:55 PM Jan 4th from API

factoring_bot

素因数分解ボット「ふぁくたん」

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

4649 is prime!

4649 is prime! RT @k4403: 4649 本日19:40頃からfactoring_botデビューイベントが開催されます．皆様，飛天の間にご参集下さい．　#scis2010

返信

about 2 hours ago from API

factoring_bot

素因数分解ボット「ふぁくたん」

大きめの素数も見つかるよ

5863981 is prime! RT @yukacci: かっこいいロリコン。 http://www.nicovideo.jp/watch/sm5863981

返信

3:00 PM Jan 13th from API

factoring_bot

素因数分解ボット「ふぁくたん」

RSA-130だって頑張る！

1807082088687404805951656164405905566278102516769401349170127021450056662540244048387341127590812303371781887966563182013214880553969859945959745429016112616288378606757644911281006483255515724345534498646735972188403686897274408864356301263205069600999044599

返信

factoring_bot

素因数分解ボット「ふぁくたん」

注※フィクションです
理論実装の困難3的に無理です

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

k4403 2010ばかり素因数分解とか自重しる！ RT @factoring_bot 2010=2*3*5*67 RT @expl01t: [ac] 5階に展示のエニグマだん．動いてるところを見た．その筋のAさん(愛すと)曰く「エニグマじゃないんじゃない？」えええぇ！！ **#scis2010**

1 day ago from Seesmic

factoring_bot 2010=2*3*5*67 RT @expl01t: [ac] 5階に展示のエニグマだん．動いてるところを見た．その筋のAさん(愛すと)曰く「エニグマじゃないんじゃない？」えええぇ！！ **#scis2010**

1 day ago from API

factoring_bot 2010=2*3*5*67 RT @k4403: おやおや？IDベース暗号を使った発表が多いぞ？ **#scis2010**

1 day ago from API

factoring_bot 2010=2*3*5*67 RT @akirakanaoka: IDベースの鍵は変えなくていいんじゃろかい？ (1E2-2) **#scis2010**

1 day ago from API

返信

factoring_bot 2010=2*3*5*67 RT @akirakanaoka: 質問したかったけど時間切れ！あああ。(1E2-2) **#scis2010**

1 day ago from API

expl01t [ac] 5階に展示のエニグマだん．動いてるところを見た．その筋のAさん(愛すと)曰く「エニグマじゃないんじゃない？」えええぇ！！ **#scis2010**

1 day ago from web

今後の課題

1. Public TLの利用
   - Streaming APIの利用？
2. GAE (PaaS)への移設
   - Pythonへの移植
   - もっと長い数字を素因数分解する！

返信

k4403

4403

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

理論と実装のギャップ（仮）

identifiableならそれがID
ぼく4403

返信

k4403
4403

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

Call for Icons

ふぁくたんのアイコンを募集しています

要求：

素因数分解っぽいアイコン

応募先：

k4403まで@かdで

返信